

# РАБОЧИЙ ДОКУМЕНТ

## Общественные риски и потенциальные гуманитарные последствия операций в киберпространстве

ПИА ХУШ и ХЕННИНГ ЛАМАНН  
ИЮНЬ 2022 г.

# ОГЛАВЛЕНИЕ

|                                                                   |    |
|-------------------------------------------------------------------|----|
| Аннотация.....                                                    | 1  |
| I. Введение .....                                                 | 3  |
| II. Субъекты кибератак.....                                       | 3  |
| 1.1. Государства.....                                             | 3  |
| 1.2. Прокси-субъекты .....                                        | 4  |
| 1.3. Независимые частные субъекты .....                           | 4  |
| III. Методы .....                                                 | 5  |
| 2.1. Программы-вымогатели и другие вредоносные программы.....     | 5  |
| 2.2. Информационные операции .....                                | 6  |
| 2.3. Атаки через цепочки поставок.....                            | 7  |
| 2.4. Кибероперации в поддержку традиционных военных операций..... | 7  |
| 2.5. Сбор разведданных и шпионаж.....                             | 9  |
| IV. Цели.....                                                     | 9  |
| 3.1. Операции против общества .....                               | 10 |
| 3.2. Операции по подрыву доверия .....                            | 11 |
| 3.3. Операции с целью нанесения физического ущерба .....          | 11 |
| 3.4. Операции с целью воздействия на данные.....                  | 12 |
| V. Уязвимости. ....                                               | 13 |
| 4.1. Физические лица.....                                         | 13 |
| 4.2. Частный сектор .....                                         | 13 |
| 4.3. Госсектор и критическая инфраструктура .....                 | 14 |
| 4.4. Общество .....                                               | 16 |
| VI. Устойчивость.....                                             | 19 |
| 5.1. Упреждающие меры.....                                        | 19 |
| Меры безопасности и защиты.....                                   | 19 |
| Меры по снижению уязвимости к дезинформации.....                  | 20 |
| Готовность на уровне общества.....                                | 20 |
| 5.2. Атрибуция.....                                               | 20 |
| 5.3. Восстановление .....                                         | 21 |
| VII. Выводы о применимых нормах права.....                        | 22 |
| Приложение 1: Список экспертов .....                              | 24 |
| Приложение 2: Установочные вопросы .....                          | 26 |
| Приложение 3: Справочный документ .....                           | 28 |

## АННОТАЦИЯ

1. Частные и государственные субъекты кибератак действуют все более умело и изощренно. Активность государств в киберпространстве может рассматриваться как возврат к «соперничеству великих держав». Для проведения своих киберопераций они нередко привлекают прокси-субъектов, выполняющих работу от их имени, тем самым вместе с работой на этих субъектов перекладывается часть рисков. Контингент независимых частных субъектов состоит преимущественно из киберпреступников, которые руководствуются прежде всего финансовыми мотивами. Методы их деятельности усложнились, они сформировали обширный и привлекательный черный рынок данных и услуг.
2. Можно выделить ряд тенденций в методах проведения враждебных киберопераций, в том числе: рост числа самопроизвольно распространяющихся вредоносных программ и разведывательных операций; все более частые случаи обхода двухфакторной аутентификации; применение искусственного интеллекта в наступательных операциях в киберпространстве; информационные операции (напр., с целью создания дипфейков); профессионализация черного рынка.
  - a. Атаки в целях вымогательства стали более изощренными, часто они непосредственно нацелены на определенные компании и учреждения; кроме того, стали чаще применяться угрозы опубликовать похищенные в ходе таких операций данные.
  - b. Информационные операции вызывают особые опасения; однако они по-прежнему не поддаются точному определению и, кроме того, отличаются от киберопераций в ряде важных аспектов, что не позволяет в борьбе с ними ограничиваться лишь мерами информационной безопасности.
  - c. Атаки через цепочки поставок создают значительный риск, в особенности это касается компаний, работающих в области высоких технологий и разработки программного обеспечения.
  - d. Кибероперации в поддержку традиционных военных операций во время вооруженных конфликтов практикуются в последние годы рядом стран. Аналогично операциям мирного времени, они в целом направлены на сбор разведывательной информации и дезорганизацию. Однако они имеют потенциально более тяжелые последствия для гражданского населения, чем в мирное время, так как сам характер конфликта может побуждать тех, кто принимает военные решения, действовать с меньшей осторожностью. Кроме того, гражданское население нуждается в гражданской инфраструктуре, которая может быть уязвимее военных систем, что делает ее привлекательной целью для киберопераций – как законных, так и незаконных.
3. При осуществлении киберопераций могут ставиться самые разные задачи, но особенно опасны те из них, которые направлены против общества в целом или имеют целью подорвать доверие к общественным институтам. Антиобщественные операции – например, нарушение работы жизненно важных служб и инфраструктуры в течение продолжительного периода – трудно осуществимы. Напротив, операции по подрыву доверия могут быть очень эффективны, и бороться с их последствиями бывает нелегко. На сегодняшний день операции против физических объектов фиксируются относительно реже.



- 4.** Степень воздействия киберопераций в значительной мере зависит от уязвимостей объекта атаки и от последствий нарушения работы такого объекта. Частный сектор крайне уязвим в тех случаях, когда переход на цифровые технологии происходит быстро и без необходимых мер предосторожности или когда связанная с ним инфраструктура информационной безопасности недостаточно развита и/или недофинансирована. Те же соображения справедливы в отношении государственного сектора и критической инфраструктуры. Уязвимость общества в целом во многом зависит от достигнутого им уровня технологической интеграции, так как при усилении сетевой взаимосвязанности возрастает риск возникновения более серьезного ущерба в результате киберинцидентов. Повышенная уязвимость общества имеет место, когда оно сильно зависит от одной технологии или когда определенные виды критической инфраструктуры представляют собой единичные точки отказа.
- 5.** Пандемия Covid-19 служит примером того, как внешние факторы могут повлиять на общественные риски и уязвимости, возникающие в результате киберопераций. Помимо прочего, риски значительно усилились в связи с ускоренным переходом компаний на электронные каналы взаимодействия, зачастую без достаточной подготовки к защите от сопутствующих рисков. Кроме того, этот опыт показал, насколько уязвима система здравоохранения к враждебным действиям в киберпространстве и к дезинформационным кампаниям.
- 6.** Степень воздействия киберопераций также зависит от того, насколько устойчив сам объект атаки. Для повышения устойчивости может быть принят ряд мер.

  - a.** Могут быть предприняты шаги для предотвращения враждебных киберопераций. К ним относятся меры безопасности и защиты, в том числе своевременное обновление программного обеспечения и применение передовых технологий, таких как системы обнаружения вторжений на основе искусственного интеллекта. Важным фактором является обеспечение всеобщей информированности и внедрение в практику адекватных правил кибергигиены. Международные механизмы защиты и более интенсивное сотрудничество между государственным сектором и частными компаниями также играют роль в повышении устойчивости к угрозам кибербезопасности.
  - b.** Другие шаги по повышению устойчивости касаются того, насколько общество подвержено воздействию дезинформационных кампаний. Там, где школьникам с ранних лет прививают медиаграмотность, уязвимость снижается. В целом общество становится менее уязвимым, когда население просвещают в вопросах кибербезопасности и разъясняют потенциальные последствия атак, а планы экстренного реагирования реализуются и доводятся до сведения широкого круга лиц с упреждением, до наступления какого-либо крупного инцидента информационной безопасности.
  - c.** Атрибуция остается непростой задачей и требует больших затрат времени, несмотря на возросшие в целом возможности. Ценность атрибуции как средства сдерживания злоумышленников по-прежнему оспаривается. В свете того аргумента, что достоверность атрибуции во многом зависит от того, кто именно делает заявление об источнике угрозы, имеет смысл продумать нейтральный и независимый, не связанный с государством механизм установления фактов, хотя создание такого механизма представляется проблематичным.

Восстановление позволяет еще больше ослабить негативные последствия киберопераций, для этого может потребоваться принятие различных мер, в частности, регулярное резервное копирование данных.



# I. ВВЕДЕНИЕ

Настоящий доклад составлен в рамках проекта «Цифровизация конфликта: Гуманитарные последствия и правовая защита» - совместной инициативы Международного комитета Красного Креста (МККК) и Швейцарской кафедры МГП Женевской академии международного гуманитарного права и прав человека. Его задача - исследовать гуманитарные последствия и потребности в защите, возникающие вследствие цифровизации вооруженных конфликтов, а также определить степень, в которой эти потребности покрываются нормами международного права, в особенности международного гуманитарного права (МГП). Совместная инициатива базируется на мультидисциплинарном подходе, в котором рассматриваются взаимосвязанные технические, военные, этические, политические, правовые и гуманитарные аспекты для ответа на три всеобъемлющих вопроса:

1. Какие риски, потенциальные гуманитарные последствия и потребности в защите затронутого конфликтом населения возникают при ведении войн в цифровом пространстве?
2. Обеспечивают ли нормы международного права, в особенности МГП, эффективное снижение этих рисков и удовлетворение этих потребностей в защите?
3. Если нет, какие могут быть выработаны рекомендации в сфере права и политики за рамками действующих норм МГП для снижения этих рисков и обеспечения этих потребностей в защите?

С февраля по май 2021 г. были проведены два экспертных семинара и четыре раунда индивидуальных консультаций с экспертами по ряду аспектов первого из этих вопросов. К участию были приглашены выдающиеся эксперты из разных стран, обладающие компетенцией в различных теоретических и практических дисциплинах, имеющих отношение к изучаемой тематике. Общая цель семинаров и консультаций состояла в том, чтобы дать актуальную оценку

существующих рисков и потребностей в защите в свете современных и будущих военных кибервозможностей. В значительной мере эти усилия опирались на предшествующую работу МККК в этой области.<sup>1</sup>

В настоящем докладе кратко представлены итоги этих консультаций. Будучи адресован прежде всего лицам, принимающим политические решения, ученым, исследователям и юристам, он имеет целью дать исчерпывающий обзор последних тенденций в сфере международной кибербезопасности и киберконфликтов. С учетом этой задачи доклад разбит на шесть взаимосвязанных разделов. В каждом из первых пяти описываются и анализируются значимые процессы последнего времени для ответа на ключевые вопросы, относящиеся к проблематике современных киберконфликтов: (1) Какие *субъекты* причастны к совершению враждебных киберопераций? (2) К каким *методам* они прибегают? (3) Каковы *цели* таких операций? (4) От чего зависят *уязвимости* объектов кибератак? (5) Что может быть сделано для повышения *устойчивости* к вредоносным кибероперациям? В шестом – заключительном – разделе кратко затрагиваются некоторые правовые вопросы, поднятые в ходе семинаров и заслуживающие более глубокого рассмотрения в ходе дальнейшей реализации инициативы.

## II. СУБЪЕКТЫ КИБЕРАТАК

Первый вопрос, требующий изучения в связи с кибероперациями – это характеристика субъектов. В силу структурных особенностей сетевой инфраструктуры не всегда бывает очевидно, кто именно осуществляет кибероперации и с какой целью. Можно выделить разные категории субъектов с их методами и мотивами. Это, прежде всего, государственные субъекты, с одной стороны, и киберпреступники, с другой, а также все более заметная категория прокси-субъектов, действующих в интересах государств.

<sup>1</sup> ICRC, *The Potential Human Cost of Cyber Operations* (Laurent Gisel and Lukasz Olejnik eds.) (МККК, *Потенциальные гуманитарные последствия киберопераций*) ICRC, Geneva, 2019; ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts* (Ewan Lawson and Kubo Mačák eds.) (*Недопущение вреда гражданскому населению от военных киберопераций во время вооруженных конфликтов*), ICRC, Geneva, 2021.

## 1.1. ГОСУДАРСТВА

Государства неуклонно наращивают свои возможности ведения киберопераций. По мнению некоторых экспертов, активность государств в киберпространстве означает возврат к «соперничеству великих держав», имея в виду, что ведущие мировые державы стали задействовать свой киберпотенциал, чтобы повлиять на поведение других государств. Связанная с этим тенденция – переход государств к наступательной политике в области кибербезопасности (концепция «упреждающей защиты») во взаимодействии со своими противниками в киберпространстве.<sup>2</sup> При этом некоторые эксперты отмечали, что в ряде случаев государства предпочли бы привлечь прокси-субъектов вместо того, чтобы действовать напрямую через свои военные или разведывательные структуры (см. далее раздел 1.2). Однако наступательные кибероперации с использованием передовых технологий требуют значительных экспертных знаний и ресурсов, включая высококвалифицированных специалистов, что в некоторой степени ограничивает роль частных субъектов в проведении некоторых технически сложных операций.

Отмечается также все более активное участие (невоенных) разведывательных органов, таких как ЦРУ или Управление правительственной связи Великобритании (GCHQ), в (военных) кибероперациях. Отчасти это является прямым следствием той важной роли, которую играет деятельность по сбору информации в подготовке киберопераций. Вовлечение подобных организаций еще более размывает границу между военными и гражданскими субъектами.

## 1.2. ПРОКСИ-СУБЪЕКТЫ

Как уже упоминалось, участники семинара указывали на часто встречающиеся утверждения о том, что государства прибегают к услугам негосударственных субъектов, действующих в их интересах, хотя эти утверждения оспариваются. Конкретные

<sup>2</sup> См. M.P. Fischerkeller and R.J. Harknett, *Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation (Постоянная вовлеченность, согласованное соперничество, динамика и эскалация взаимодействий в киберпространстве)*, (2019) *Cyber Defense Review* 267.

задачи, которые предположительно берут на себя такие субъекты, варьируются от разработки средств эксплуатации уязвимостей до фактического использования обнаруженных уязвимостей и внедрения вредоносного кода – то есть, проведения наступательных киберопераций в полном объеме. Спонсируя такие частные структуры, государства могут не только передавать подрядчикам необходимые виды работ, но и частично перекладывать на них риск. Такой аутсорсинг может быть привлекательным, поскольку в этом случае атрибуция с достаточным объемом доказательств затруднена, что позволяет ведущему операцию государству избегать правовой и политической ответственности за свои действия. Однако привлечение прокси-субъектов также сопряжено с риском, так как у них могут быть или появиться собственные мотивы для злонамеренных действий в киберпространстве, что сделает трудным контроль за ними со стороны нанявшего их государства.

## 1.3 НЕЗАВИСИМЫЕ ЧАСТНЫЕ СУБЪЕКТЫ

В полном смысле частные – т. е. негосударственные и не действующие в интересах государства – субъекты отличаются от государственных субъектов по ряду параметров. Наибольшее значение имеет тот факт, что их деятельность часто направлена на получение финансовой выгоды. Это предполагает, что, в отличие от государств, такие субъекты в большинстве случаев не преследуют политических целей, осуществляя наступательные кибероперации.

В последнее время некоторые частные субъекты стали действовать более изощренно. Особо следует отметить все более распространенную модель поведения, которая отражает степень профессионализма киберпреступников: речь идет о так называемых разведывательных атаках, когда добытые личные данные не используются самим злоумышленником, а продаются в теневом сегменте интернета. Похищенная таким образом информация часто представляет собой учетные данные пользователей, а также сведения об уязвимости ИТ-систем и средства доступа к уже инфицированным системам. Эта категория субъектов может быть определена как «брокеры начального доступа». Все это приводит к значительному сокращению сроков проведения наступательных киберопераций и увеличению их масштабов.

Чтобы адекватно реагировать на эту растущую профессионализацию, необходимо наращивать усилия в области кибербезопасности и киберзащиты. По мере того, как общество осознает потребность в более надежных средствах обеспечения кибербезопасности как в государственном, так и в частном секторе, создаются дополнительные вакансии, хотя многие из них остаются незанятыми из-за нехватки квалифицированных и опытных кандидатов.<sup>3</sup>

При этом общий уровень компетенций и технических знаний в сфере ИТ, которые необходимы для совершения таких преступных деяний, остается относительно невысоким. Некоторые эксперты указывают, что преступные кибероперации создают большой риск для жизни и здоровья людей, чем операции, организуемые национальными государствами, поскольку направлены обычно против гражданских компаний и лиц или проводятся безответственно и неизбирательно.

Еще одной проблемой, относящейся к кибербезопасности, является угроза внутренних атак. Несмотря на постоянный рост числа субъектов, представляющих угрозу, правоохранительным органам в целом удается идентифицировать киберпреступников. Благодаря этому все большее число известных злоумышленников вносятся в списки лиц, разыскиваемых полицией, что сильно ограничивает для них возможность совершать поездки, не рискуя подвергнуться аресту.

### III. МЕТОДЫ

При нынешних темпах технологического прогресса быстрое развитие технологий происходит и в сфере киберконфликтов. Тем не менее, можно выделить несколько очевидных тенденций, относящихся к методам совершения киберопераций. Во-первых, участилось применение так называемых самораспространяющихся вредоносных программ, а именно червей и вирусов, которые преобладают при совершении атак на ИТ-системы и применяются значительно чаще таких методов, как внедрение троянских программ

или кража паролей. Как следует из самого термина, такие вредоносные программы способны самопроизвольно переходить из одной системы в другую, причем этот процесс может продолжаться годами после первичного внедрения. Вследствие этого они остаются источником потенциального риска в течение длительного времени. Большинство вредоносных программ удаляются в процессе переустановки операционной системы компьютера, хотя существуют версии, устойчивые даже к таким радикальным мерам.<sup>4</sup>

Напротив, стали реже применяться троянские программы, которые маскируются под обычное ПО, но внедряются в атакуемую систему, чтобы после активации отслеживать ее активность или эксплуатировать ее иным образом. Во-вторых, наблюдается резкий рост разведывательных операций (см. выше раздел 1.3). Это связано с третьей тенденцией – участившимися случаями обхода двухфакторной аутентификации. Например, хакеры могут задействовать функцию восстановления пароля или обойти второй этап аутентификации, подобрав четырехзначный или шестизначный код путем простого перебора комбинаций. В-четвертых, значительно участились случаи масштабной утечки данных. Наконец, все активнее применяется искусственный интеллект, в том числе при проведении наступательных киберопераций и информационных операций. (напр., при создании дипфейков).

Кибероперации, приводящие к физическому разрушению объекта атаки, остаются редким явлением, и не в последнюю очередь из-за их сложности. При этом не следует приравнивать степень изощренности операции к ее результативности. Более того, вредное воздействие может также достигаться с помощью операций, проведение которых не требует каких-либо сложных приготовлений технического или практического характера.

Отмечалось, что (черный) рынок существенно вырос в масштабах, что он стал более профессиональным и что на нем можно легко приобрести данные, относящиеся к безопасности, включая пароли, как легально, так и нелегально, так как рынок по большей части остается вне сферы регулирования. Один из экспертов выразил мнение, что западные государства неосознанно

<sup>3</sup> См., напр., William Crumpler & James A. Lewis, *The Cybersecurity Workforce Gap (Кадровый разрыв в сфере кибербезопасности)*, 29 января 2019, <https://www.csis.org/analysis/cybersecurity-workforce-gap>.

<sup>4</sup> См. Michael Kan, *Suspected Chinese Hackers Unleash Malware That Can Survive OS Reinstalls (Предполагаемые китайские хакеры запустили вредонос, способный сохраняться при переустановке ОС)*, PC Mag, 5 октября 2020 г.,



поддерживают такой рынок, ускоряя гонку кибервооружений, при этом оставляя его в значительной мере без регулирования. Имея доступ к этому рынку, злоумышленники могут использовать его для нанесения существенного ущерба.

## 2.1. ПРОГРАММЫ-ВЫМОГАТЕЛИ И ДРУГИЕ ВРЕДНОСНЫЕ ПРОГРАММЫ

Неуклонный рост числа вымогательских кибератак – пожалуй, наиболее четко прослеживаемая тенденция. Можно выделить два основных варианта этого типа наступательных киберопераций. С одной стороны, это оппортунистические операции, осуществляемые путем неизбирательного распространения программ-вымогателей. С другой стороны, с недавнего времени наблюдается тенденция к целенаправленному применению таких программ под прямым контролем человека. Хотя целенаправленные вымогательские атаки часто оказываются более выгодными по сравнению с оппортунистическими, они могут проводиться и в целях политического шантажа, а не только по чисто материальным соображениям. Они также применяются в ситуациях, когда доступ к атакуемому объекту особенно затруднен, как в случае установки специализированных и, как правило, хорошо защищенных промышленных систем управления элементами критической инфраструктуры, к каковым относятся, например, электростанции.<sup>5</sup>

В последние годы обращает на себя внимание постепенная профессионализация атак с помощью программ-вымогателей, особенно это касается разведывательной деятельности при подготовке целевых операций. В то же время, наблюдается рост числа фишинговых атак, и хотя такие операции часто не дают немедленного эффекта, они могут приводить к ущербу и

другим негативным последствиям спустя некоторое время. Кроме того, все большее распространение находит практика двойного вымогательства в контексте хищения данных. Это означает, что, помимо угрозы уничтожения данных или их изменения, данные «берутся в заложники», в то время как злоумышленники угрожают осуществить их утечку, если не получат выкуп. Объектами таких атак все чаще становятся крупные компании и в меньшей степени – «оппортунистические» цели. Эта тенденция также означает, что целенаправленные операции часто готовятся заранее, в течение нескольких месяцев, чтобы собрать достаточное количество информации на предварительных этапах. Еще одним аспектом профессионализации вымогательских операций сравнительно недавно стали коммерческие предложения так называемого «взлома как услуги», размещаемые в теневом сегменте интернета. Такие услуги могут предусматривать различные схемы монетизации; например, хакеры, выступающие в роли «брокеров начального доступа», могут предлагать клиентам доступ к системе-цели, а не проводить самостоятельно всю операцию с использованием программы-вымогателя.

Помимо вышеописанной деятельности киберпреступников, операции с применением программ-вымогателей могут проводиться в военных целях. Заинтересованность военных в подобных операциях обычно не связана с получением денежной выгоды. Скорее государства могут стремиться создать видимость, что вымогательская операция была предпринята киберпреступниками, тем самым используя данный образ действий прежде всего как прикрытие, чтобы отвлечь внимание от других мотивов и затруднить атрибуцию. Такие операции фактически могут иметь целью удалить массивы данных, одновременно нанеся необратимое физическое повреждение устройствам хранения, чтобы затруднить атакуемой стороне восстановление систем с помощью средств резервирования, или нарушить работу резервных дата-центров, сделав их непосредственной целью киберопераций.

## 2.2. ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ

Еще одна значимая тенденция – рост числа информационных операций, построенных на цифровых технологиях. Хотя информационные

<sup>5</sup> Следует отметить, что не все элементы критической инфраструктуры труднодоступны сами по себе. В 2017 г. Национальная система здравоохранения (NHS) Великобритании подверглась массовой кибератаке. В то время в ведомстве использовалась ОС Windows 7 OS, что делало его относительно уязвимым. См. National Audit Office, Investigation: WannaCry cyber-attack and the NHS (Национальное контрольно-ревизионное управление, расследование: Кибератака с помощью вируса WannaCry и NHS, 27 октября 2017 г., <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/>).

операции всегда имели место в той или иной форме, то, насколько быстрее могут быть достигнуты цели и получены результаты информационных операций при использовании цифровых средств, не может не вызывать беспокойство. Особенно тревожной представляется вошедшее недавно в практику применение технологий на основе искусственного интеллекта при проведении информационных операций – например, для создания сфабрикованных цифровых видеоматериалов. В принципе, информационные операции не требуют больших ресурсов, в отличие от сложных киберопераций, хотя в некоторых вариантах все же могут задействоваться значительные ресурсы, которые доступны не всем субъектам.

Трудности возникли в решении вопроса о том, как определить и идентифицировать «информационные операции в киберпространстве». Рассмотрим пример использования ботов в социальных сетях; в ходе консультаций не удалось прийти к единому мнению относительно того, подпадает ли данный случай под определение «информационных операций в киберпространстве». По мнению некоторых экспертов, даже в отношении таких традиционных средств массовой информации, как BBC или CNN, значительно расширивших свою аудиторию с помощью сетевых ресурсов, можно сказать, что они проводят информационные кибероперации, которые оказывают влияние на внутренние дела других – в особенности незападных – государств.

Кроме того, трудность с определением и идентификацией информационных операций означает, что успешную стратегию защиты труднее реализовать, поскольку главная проблема заключается не в самой используемой технологии, а в том, *как* она используется для донесения информации до людей. Дополнительным фактором, требующим рассмотрения, является право на свободу выражения мнений. Меры, направленные на борьбу с угрозой информационных операций, следует проводить с осторожностью, чтобы не допустить неоправданного нарушения этого права человека.

Важно отметить, что информационные операции концептуально отличаются от других киберопераций тем, что их объектом

становится человеческая психология, а не компьютерные системы или физические активы (см. также далее разделы 3.2 и 4.3). Не в последнюю очередь в силу этого определяющего качества противодействие информационным операциям (независимо от того, насколько точным является их описание как «проводимых в киберпространстве») не является проблемой кибербезопасности в ее истинном понимании.

Наконец, информационные операции могут также играть существенную роль во время вооруженных конфликтов – например, как средство поддержки традиционных военных операций. Экспертами высказывалась озабоченность в связи с далеко идущими разрушительными последствиями информационных операций не только в период активных боевых действий, но и в постконфликтных ситуациях. В частности, информационные операции, направленные на подрыв доверия к обществу и институтам, были названы в качестве особенно серьезной проблемы в этом контексте (см. далее раздел 3.2).

## 2.3. АТАКИ ЧЕРЕЗ ЦЕПОЧКИ ПОСТАВОК

Хотя наступательные кибероперации, направленные против программных и аппаратных цепочек поставок, остаются достаточно редким явлением, их число в последнее время выросло. Такие атаки через цепочки поставок совершаются в основном путем проникновения в целевую систему через продукт, предоставляемый третьей стороной (например, поставщиком ПО или аппаратных средств), которая на законных основаниях осуществляет права доступа к целевой системе и к связанным с ней данным. Этот вид злонамеренных действий вызывает опасения ввиду потенциально разрушительных последствий для деятельности высокотехнологичных компаний, компаний по разработке программного обеспечения, а также для секторов критической инфраструктуры, включая энергетику – особенно для поставщиков электроэнергии и природного газа. Что еще более важно, атаки через цепочки поставок часто затрагивают продукты, используемые для мониторинга и поддержания безопасности несколькими компаниями. Если злоумышленнику удастся скомпрометировать базу исходного кода ПО, используемого несколькими крупными компаниями (например,

операционной системы или промышленной системы управления), он получает доступ сразу к нескольким объектам атаки. Это затрудняет оценку потенциальных последствий. В этом контексте инцидент с компанией SolarWinds являет собой тревожный пример далеко идущих последствий, которые могут иметь кибератаки через цепочки поставок.<sup>6</sup>

Наряду с прямым воздействием на деятельность подвергшихся нападению организаций атаки через цепочки поставок могут порождать серьезный и долгосрочный эффект системного характера. Цепочки поставок аппаратных средств и программного обеспечения строятся на взаимном доверии между поставщиками и их клиентами – конечными потребителями – не только при поставке новых продуктов, но также, что особенно важно, в связи с необходимостью частого обновления программ и систем. С ростом числа атак через цепочки поставок это жизненно важное доверие неизбежно ослабевает, что грозит скомпрометировать всю существующую систему цепочек поставок, от которой зависят как частные экономические субъекты, так и государственные учреждения.

## 2.4. КИБЕРОПЕРАЦИИ В ПОДДЕРЖКУ ТРАДИЦИОННЫХ ВОЕННЫХ ОПЕРАЦИЙ

Осуществление масштабной кибератаки в масштабах всей страны представляется маловероятным. Во всяком случае, эксперты выразили сомнение в возможности поддерживать такую атаку продолжительное время, сосредоточив ее на определенном объекте, в сочетании с намерением нарушить работу нескольких систем одновременно. Тем не менее, насколько можно судить, некоторые кибероперации в поддержку традиционных военных операций имели место – в частности, кибероперации ряда западных стран против центра командования и управления группировки «Исламское Государство», предпринятые параллельно с усилиями по нейтрализации ее пропагандистской стратегии.<sup>7</sup>

<sup>6</sup> См. Julia Kisielius, Breaking Down the SolarWinds Supply Chain Attack (Разбор кибератаки на цепочку поставок SolarWinds), SpyCloud, 11 марта 2021 г., <https://spycloud.com/solarwinds-attack-breakdown/>.

Кибероперации в поддержку традиционных военных операций также могут быть направлены против комплексов вооружения с целью выведения их из строя. Хотя в таких операциях трудно достичь успеха, комплексы вооружения, которые являются устаревшими и, как следствие, имеют уязвимости в системах управления, могут стать выгодными целями для противника.<sup>8</sup> Как упоминалось ранее, (см. раздел 2.1), среди используемых методов могут также быть кибероперации, имеющие целью шифрование данных противника. Еще один аспект современной войны, заслуживающий внимания в данном контексте – это возможность нарушить военную спутниковую связь посредством киберопераций. Имеется в виду проведение киберопераций против наземных станций или линий связи в сочетании с поражением спутников с помощью кинетического оружия. Такие операции могли бы иметь особенно разрушительные последствия и обеспечить атакующей стороне значительное военное преимущество, например, при подавлении сигналов GPS. Однако такая масштабная операция с нарушением спутниковой связи почти наверняка будет иметь тяжелые последствия для гражданского населения, а также для третьих сторон, не участвующих в вооруженном конфликте.

В этом контексте представляются важными еще два соображения, выходящие за рамки конкретных операций. Один из экспертов отметил, что для нанесения противнику планируемого поражения сложные военные кибероперации часто требуют усиленного сбора

<sup>7</sup> См. Deborah Haynes, Into the Grey Zone: The 'offensive cyber' used to confuse Islamic State militants and prevent drone attacks (Применение «наступательных киберсредств» для дезориентации боевиков «Исламского государства» и предотвращения атак дронов), 8 февраля 2021 г., <https://news.sky.com/story/into-the-grey-zone-the-offensive-cyber-used-to-confuse-islamic-state-militants-and-prevent-drone-attacks-12211740> (интервью с двумя высокопоставленными должностными лицами Великобритании). К числу стран, признавших применение киберопераций во время вооруженных конфликтов также относятся США ([https://www.armed-services.senate.gov/imo/media/doc/Nakasone\\_02-14-19.pdf](https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf)) и Франция ([https://www.lemonde.fr/international/article/2019/07/12/general-lecointre-l-indicateur-de-reussite-n-est-pas-le-nombre-de-djihadistes-tues\\_5488379\\_3210.html](https://www.lemonde.fr/international/article/2019/07/12/general-lecointre-l-indicateur-de-reussite-n-est-pas-le-nombre-de-djihadistes-tues_5488379_3210.html)).

<sup>8</sup> См. Lukasz Olejnik, The Dire Possibility of Cyberattacks on Weapons Systems (Зловещая возможность проведения кибератак на комплексы вооружений), Wired, 10 марта 2021 г., <https://www.wired.com/story/dire-possibility-cyberattacks-weapons-systems/>.

разведывательной информации в мирное время, до начала вооруженного конфликта. По этой причине деятели, ответственные за принятие решений, считают необходимым обеспечить свое присутствие в системах противника, чтобы быть готовыми к проведению военных киберопераций, когда это потребуется – практика, известная как «подготовка боевых действий» в киберпространстве.<sup>9</sup>

Как в традиционных военных операциях, так и в обеспечивающих их кибероперациях присутствуют одни и те же факторы планирования. Процессы изменения и модернизации вооруженных сил в целом, равно как и киберпотенциала, обеспечивающего традиционные военные операции, предполагают более интенсивное использование военными гражданской инфраструктуры и соответствующих служб, например, для поддержания цепочек поставок и элементов критической инфраструктуры. Кроме того, ускорение темпов проведения операций может приводить к тому, что меньше времени будет оставаться на разведку и маневрирование и, как следствие, на принятие мер предосторожности, чтобы удостовериться в том, что выбранные цели подпадают под определение военных объектов и что нападение на них не запрещено нормами МГП.<sup>10</sup>

Кроме того, выбор киберопераций, проводимых в поддержку военных операций, часто диктуется тем, насколько эффективны они в решении определенной военной задачи. Например, если необходимо сбить военный самолет противника, такую боевую задачу трудно выполнить непосредственно с помощью киберопераций. Однако кибероперации могут результативно применяться для атак на службы управления воздушным движением или для перехвата управления беспилотным

летательным аппаратом. Поэтому при использовании киберопераций в поддержку военных операций первым шагом обычно является поиск уязвимых целей. К сожалению, это означает, что атака на гражданские объекты часто рассматривается как путь наименьшего сопротивления, что ведет к дальнейшему усугублению общественных рисков и потенциальных гуманитарных последствий киберопераций во время вооруженных конфликтов. Для государства, однако, выбор киберопераций как альтернативы непосредственному участию в военном конфликте может означать более устойчивую поддержку населением его военных усилий, поскольку меньше человеческих жизней подвергается прямому риску.

В целом кибероперации во время конфликта существенно не отличаются от таких же операций в мирное время, и, в принципе, осуществляются теми же методами и средствами. Как в мирное время, так и во время конфликта кибероперации решают две общие задачи: сбор разведывательной информации и дезорганизация работы объектов. Имеют место различия в выборе целей, но следует ожидать трудностей в разграничении гражданских и военных объектов, поскольку типичная киберинфраструктура включает значительное число объектов двойного назначения. С учетом этого факта некоторые эксперты утверждали, что кибероперации, осуществляемые во время вооруженных конфликтов, могут приводить к более тяжелым последствиям для гражданского населения, чем подобные операции в мирное время, так как сам характер конфликта может побуждать лиц, принимающих военные решения, действовать с меньшей осмотрительностью в отношении гражданской инфраструктуры и имущества, а это значит, что операции будут иметь менее предсказуемые последствия. Как можно видеть на примере Украины, по электросетям одной из сторон конфликта могут наноситься удары без должного учета жизненно важных гражданских служб, зависящих от электроснабжения.

## 2.5. СБОР РАЗВЕДАННЫХ И ШПИОНАЖ

Сбор разведывательной информации представляет собой важнейший этап подготовки киберопераций. Например, часто сбор информации закладывает основу для информационной операции, но также и для «подготовки боевых действий», поскольку эффективное проведение масштабных или в ином

<sup>9</sup> См. Karl Grindal and Karim Farhat, *Persistent Engagement or Preparing the Battlefield? (Постоянная вовлеченность или подготовка боевых действий?)*, Internet Governance Project, 24 июня 2019 г., <https://www.internetgovernance.org/2019/06/24/persistent-engagement-or-preparing-the-battlefield/>.

<sup>10</sup> См. (ст. 57/2/a/i I ДП), признанную отражающей обычное международное право (Норма 16 Исследования «Обычное МГП»). См. общую информацию в материале ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts (Недопущение вреда гражданскому населению от военных киберопераций во время вооруженных конфликтов)* (под ред. Ewan Lawson и Kubo Mačák), ICRC, Geneva, 2021.



отношении сложных военных киберопераций обычно требует усиленного или даже почти непрерывного предварительного сбора информации, например, для обнаружения слабых мест и уязвимостей в системах противника и для анализа возможностей совершения враждебных действий, в том числе во время таких кризисов, как глобальная пандемия. Кроме того, сбор разведанных необходим для повышения точности при проведении киберопераций, не в последнюю очередь во избежание вреда гражданскому населению или гражданской инфраструктуре. В то же время объем (личных) данных, собираемых методами разведки, поднимает вопросы в области прав человека, относящиеся к праву на неприкосновенность частной жизни и праву на защиту данных. Наконец, следует отметить, что кибероперации, проводимые для подготовки боевых действий, обычно не сводятся к простому сбору разведанных и часто включают внедрение в системы противника вредоносных программ, которые впоследствии могут быть активированы («превращены в оружие»), если в этом возникнет необходимость.

В сущности, сбор разведанных, о котором шла речь выше, является подкатегорией традиционного шпионажа. При том, что шпионаж как таковой не признан незаконным в соответствии с международным правом, встает вопрос: должен ли шпионаж в контексте военных киберопераций быть отнесен к другой категории с правовой точки зрения, особенно если его цель – подготовка боевых действий? С технической точки зрения эта деятельность тоже должна рассматриваться как выходящая за рамки простого сбора разведанных или «простого шпионажа», так как может оказывать непреднамеренное парализующее воздействие на систему, даже при отсутствии других действий, таких как кража данных извне. Со своей стороны, операторам атакованной сети необходимо выделять ресурсы и время для расследования инцидента, который мог привести к неработоспособности систем. Более того, объемы извлекаемых данных также существенно иные, нежели в случае традиционного шпионажа, в связи с чем возникают вопросы о том, должна ли быть пересмотрена оценка законности таких действий.

## IV. ЦЕЛИ

Кибероперации могут предприниматься для решения ряда задач. У киберпреступников преобладает мотивация финансового характера, тогда как другие кибероперации преследуют иные цели, что подразумевает другие объекты атак. Особые опасения связаны с теми операциями, которые направлены против общества в целом (раздел 3.1) или имеют целью подрыв доверия (раздел 3.2). В целом в последние годы среди кибердержав наблюдается тенденция к совершению атак на процессы, жизненно важные для функционирования общества, а не на цели ограниченных масштабов (такие как системы управления производственными процессами отдельно взятого предприятия с целью физического воздействия).<sup>11</sup> Операции могут быть легче идентифицированы, если они имеют целью нанесение физического ущерба (см. раздел 3.3) или воздействие на данные (раздел 3.4). Первые два типа операций несут в себе особенно значительные риски и вызывают последствия, которые сложнее оценить и измерить.

### 3.1. ОПЕРАЦИИ ПРОТИВ ОБЩЕСТВА

Кибероперации, с которыми связывают особые опасения – это операции, направленные против общества в целом и имеющие целью его дестабилизировать, например, путем вмешательства в важнейшие общественные процессы – голосование, налогообложение, образование – или их нарушения. Такое обширное воздействие с далеко идущими последствиями для всего общества может достигаться, например, путем проведения наступательных киберопераций против инфраструктуры, которая обеспечивает жизненно важные услуги, или комплексных

<sup>11</sup> См. подробнее Robin Geiss and Henning Lahmann, *Protecting Societies: Anchoring a New Protection Dimension in International Law in Times of Increased Cyber Threats*, Geneva Academy Working Paper Series, February 2021 (*Защита обществ: Закрепление нового аспекта защиты в международном праве во времена усилившихся киберугроз. Серия рабочих документов Женевской академии, февраль 2021 г.*), <https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchoring.pdf>.

информационных операций, направленных на подрыв доверия к общественным институтам. (см. также содержание раздела 3.2 ниже). Вместе с тем, эксперты высказали сомнения в отношении вероятности того, что военная кибероперация может иметь устойчивые и масштабные общественные последствия вплоть до «развала» всего общества путем применения кибернетических сил. Такое воздействие – во всяком случае, долговременное – труднодостижимо, учитывая, что люди способны адаптироваться к кризисам. Для реализации такой цели потребовался бы ряд скоординированных операций, что представляется менее реальной угрозой в ближайшей перспективе.

В этом контексте кибероперации на территории Украины в 2014 г. обсуждались как пример того, как такие операции могут повлиять на общество в целом. В данном случае кибероперации, предпринятые в попытке парализовать сетевую инфраструктуру в Украине, были успешно скоординированы непосредственно перед тем, как танки пересекли границу. Таким образом, кибероперации с очевидностью становятся компонентом других военных операций, и пример Украины показывает, что сетевая атака с целью парализовать работу интернета в отдельно взятом регионе уже была применена в качестве стратегии. Необходимо отметить при этом, что, как следует из данного примера, подобные далеко идущие системные последствия для общества часто носят лишь краткосрочный характер, однако было признано существенным, что наступательные операции, помимо прочего, затронули компьютерные системы, используемые аптечными сетями Украины для поиска лекарств, что могло затруднить гражданскому населению получение необходимых лекарственных средств. Эти последствия, как минимум, указывают на потенциальную опасность этого типа киберопераций, нацеленных на такие жизненно важные социальные функции, как сетевая инфраструктура.

Как упоминалось ранее, особенно серьезные опасения были высказаны в связи с информационными операциями, цель которых – вызвать масштабный общественный резонанс; в особенности речь идет об операциях с целью подрыва доверия

и социальной сплоченности как существенных условий функционирования современных открытых обществ. Подобные негативные последствия могут быть вызваны, например, атакой на такие ключевые общественные процессы, как выборы, нарушением работы финансовых учреждений или экономики в целом. Даже если сохранение каких-либо долговременных последствий представляется маловероятным, инструменты информационных операций способствуют попыткам достичь этих целей. Если в прошлом противник должен был выбирать между кратковременным воздействием на широкий круг объектов и более интенсивным воздействием на относительно узкую целевую группу, то сейчас такой выбор неактуален. Более того, растущая зависимость общества от электронных средств связи, использование слабо защищенных устройств, управляемых через интернет, и промышленных систем управления создает для хакеров, как минимум, потенциальную возможность усиливать системные негативные последствия для подвергаемых атакам обществ. Операции, направленные на подрыв общественного доверия, будут подробно рассмотрены в следующем разделе.

Таким образом, проведение крупных операций, способных на долгое время дестабилизировать целое общество, связано с большими трудностями. Однако в таких сложных и масштабных операциях нет необходимости, если ставится конкретная цель, так как даже небольшие многократные дезорганизующие воздействия или операции с меньшим уровнем сложности могут нанести ущерб обществу в целом.

### 3.2. ОПЕРАЦИИ ПО ПОДРЫВУ ДОВЕРИЯ

Кибероперации, направленные на подрыв доверия гражданского населения к политической системе и институтам государства, вызывают особую озабоченность. Прежде всего, такие результаты могут быть получены посредством скоординированных дезинформационных кампаний или других видов информационных операций, особенно если задействуются возможности искусственного интеллекта. Хотя масштабные операции могут достигать высокого уровня сложности, что делает их крайне ресурсоемкими, эффект ослабления сплоченности общества может достигаться

сравнительно недорогими средствами. Например, если существующие социальные сети используются для распространения дезинформации с целью повлиять на умонастроения и психологическое состояние целевой группы населения, информационные операции могут приобретать широкий охват, не требуя значительных затрат ресурсов.

В частности, с помощью информационных кампаний среди целевых групп населения может распространяться недоверие к работе финансовых учреждений и финансовой системе в целом, побуждая многих физических лиц к изъятию вкладов из банков. Это доказывает, что совсем не обязательно предпринимать атаку непосредственно на банк - тот же эффект может быть достигнут путем распространения дезинформации как относительно дешевого средства по сравнению с тщательно организованной кибероперацией по взлому, как правило, хорошо защищенных ИТ-систем финансовых учреждений. Таким образом, манипулируя поведением отдельных людей, можно добиться желаемого эффекта косвенным путем. Система выборов, которая считается «слабым звеном» среди общественных институтов, особенно уязвима к атакам, что позволяет противнику добиваться изменений в обществе относительно небольшими усилиями. Помимо возможного экономического и финансового ущерба или изменений в политике, такие факторы политической нестабильности могут приводить к массовой утрате общественного доверия, создавая экзистенциальные риски для обществ в долгосрочной перспективе. В исключительных случаях эти процессы могут даже провоцировать общественные волнения или восстания.

Особенно острую проблему в этом контексте представляет тот факт, что утрату доверия трудно оценить или измерить. Хотя некоторые аспекты можно отслеживать во времени, например, путем изучения электорального поведения, такие процессы носят скорее средне- и долгосрочный характер, и их анализ требует временных затрат. Вследствие этого оценка снижения доверия не может осуществляться теми темпами, которые необходимы для эффективного реагирования на такие информационные операции. Задача еще больше осложняется тем, что в этом

контексте причинно-следственная связь трудно доказуема.

Таким образом, утрата репутации определенными институтами может иметь потенциально более серьезные последствия по сравнению с кинетическим воздействием. Физические объекты и инфраструктура в большинстве случаев поддаются ремонту. С другой стороны, восстановить доверие бывает крайне трудно, и это возможно только со временем, если вообще возможно.

### 3.3. ОПЕРАЦИИ С ЦЕЛЬЮ НАНЕСЕНИЯ ФИЗИЧЕСКОГО УЩЕРБА

Количество киберопераций с физическим воздействием на объект в целом оказалось меньше, чем многие наблюдатели ожидали одно или два десятилетия назад. Главная причина в том, что такие операции отличаются большой сложностью, а физические объекты представляют собой трудную цель. Кроме того, государства могут быть не готовы проводить операции, связанные с физическим воздействием, поскольку для этого им пришлось бы задействовать свои самые мощные кибервозможности, которые государства не заинтересованы раскрывать, кроме как для достижения значительного стратегического преимущества. Во всех случаях, когда это возможно, государства с большей вероятностью будут в первую очередь прибегать к операциям, требующим меньше усилий и ресурсов. Аналогичным образом, если та же или подобная цель может быть достигнута другими, некибернетическими средствами, таким средствам может быть отдано предпочтение, учитывая сложность киберопераций, которые потребуются для ее достижения.

Вместе с тем, это не означает, что полностью отсутствует риск проведения в будущем киберопераций, приводящих к физическому ущербу. Хотя на сегодняшний день реализовано небольшое число операций против физических объектов, их проведение остается возможным, особенно учитывая появление множества новых средств и инструментов. Субъекты, менее компетентные в этих вопросах, но обладающие необходимым бюджетом, могли бы приобретать инструменты для наступательных киберопераций, такие как средства эксплуатации уязвимостей, вредоносные

программы, либо соответствующие услуги на черном рынке, чтобы осуществлять операции в целях нанесения масштабного физического ущерба. Хотя такой образ действий не был признан сколько-нибудь вероятным, некоторые эксперты указали на то, что его нельзя полностью исключить.

К гипотетическим примерам операций, нацеленных на физические объекты, относятся операции по уничтожению летящего самолета или операции против военного оборудования, включая комплексы вооружений (см. выше раздел 2.4). Атаки на глобальные коммуникационные системы, такие как спутниковые линии связи или навигационные системы, также могли бы иметь особенно разрушительные последствия.

Также была высказана озабоченность в связи с операциями, нацеленными на базовые интернет-службы и инфраструктуру. Один из экспертов отмечал, что, в отличие от операций, объекты которых состоят лишь из байтов и битов или из кремния и потому легко восстановимы, более сложные операции, например, против промышленных систем управления, гораздо более вредоносны по своему характеру. Такие системы необходимы для безопасного функционирования многих элементов критической инфраструктуры, в частности, электросетей, и вывод их из строя легко может приводить к такому физическому повреждению атакуемой инфраструктуры, который затрудняет ее быстрое восстановление. В результате целые города могут быть отрезаны от источников важнейших ресурсов, в том числе электричества и питьевой воды, что вызовет немалые страдания среди населения.<sup>12</sup>

Критическая инфраструктура в особенности может стать потенциальной мишенью будущих киберопераций (см. также далее раздел 4.3). В этом контексте эксперты обсудили гипотетический пример наступательной кибероперации с целью нарушения работы светофоров или систем управления железнодорожным движением, следствием чего могут быть аварии, приводящие к физическому ущербу. Однако

один из экспертов не согласился с этим, так как, по его мнению, подобное воздействие на систему управления движением поездов лишь прервало бы железнодорожное сообщение. Учитывая современные системы безопасности, установленные в такой масштабной инфраструктуре, любое воздействие будет ограничено изменением расписания поездов – несомненное неудобство, но, вовсе не представляющее угрозу физической целостности объектов или даже жизни людей.

Однако этот пример отражает еще один важный аспект: возникает вопрос, что считать физическим ущербом. Невзирая на отсутствие явной угрозы жизни и здоровью в таких сценариях, при оценке потенциального ущерба нельзя не учитывать возможные долговременные последствия, которые могут даже привести к сокращению продолжительности жизни, если нарушена работа некоторых критически важных служб.

### 3.4. ОПЕРАЦИИ С ЦЕЛЬЮ ВОЗДЕЙСТВИЯ НА ДАННЫЕ

Масштабные последствия также могут наступить, когда кибероперации проводятся с целью получения доступа к персональным или не персональным данным. Объектом атаки могут быть, например, документы медицинского или налогового учета, данные органов социального обеспечения. В этом случае манипуляция с данными может иметь более тяжелые последствия, чем просто получение доступа к ним или даже их удаление, поскольку может отсутствовать указание на то, какие именно данные были изменены и в какой степени. Такая неопределенность может усиливать недоверие со стороны граждан, в особенности по отношению к тем учреждениям, которые отвечают за управление соответствующими массивами данных – например, к налоговым органам. Хотя получение доступа к учетным данным в разведывательных целях случается нередко, сами данные обычно не подвергаются систематическому удалению, и такой шаг будет расцениваться как дальнейшая эскалация.

Ряд экспертов отмечали особую опасность масштабных утечек данных – эта тенденция, как ожидается, в дальнейшем будет нарастать. Речь идет о таких данных, как цифровые идентификаторы, включая биометрические данные, а также медицинская документация –

<sup>12</sup> См. подробно Sergio Caltagirone, *Industrial Cyber Attacks: A Humanitarian Crisis in the Making (Промышленные кибератаки: назревающий гуманитарный кризис)*, МККК, «Гуманитарное право и политика», 3 декабря 2019 г., <https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/>.



например, в результате недавней крупной утечки данных в Бразилии в свободный доступ попали личные медицинские данные 243 миллионов бразильских граждан.<sup>13</sup> Такие утечки вызывают особую тревогу, учитывая, что похищаются, в том числе, биометрические данные, которые, в отличие от паролей, не подлежат изменению; те, кого затронули подобные инциденты, рискуют стать жертвами последующих киберпреступлений, например, подвергнуться шантажу, если похищенные конфиденциальные данные попадут в руки злоумышленников.

## V. УЯЗВИМОСТИ

Однотипные действия в киберпространстве могут иметь разные последствия в зависимости от того, какие лица, общества и даже отрасли становятся объектами кибератак. Степень воздействия во многом зависит от того, насколько соответствующие объекты атаки подвержены вредоносным факторам киберопераций. Исходя из этого, эксперты обсудили факторы, которые делают некоторых лиц особенно уязвимыми к враждебным кибероперациям; также речь шла о том, какие элементы государственного или частного сектора могут столкнуться с наиболее тяжелыми последствиями, подвергнувшись атакам. Самое прямое отношение к теме этого раздела имело обсуждение вопросов, касающихся критической инфраструктуры, но затрагивались также уязвимости общества в целом. Рассмотрим последовательно соответствующие группы.

### 4.1. ФИЗИЧЕСКИЕ ЛИЦА

В зависимости от того, какие интересы затронуты, атаки непосредственно против физических лиц представляются менее вероятными, во всяком случае, когда речь идет о военных или иных проводимых государством киберопераций. Физические лица могут рассматриваться одновременно как слабейшее и сильнейшее звено в системе кибербезопасности. Хотя известно множество

примеров несоблюдения индивидуальными пользователями правил «кибергигиены» (пренебрежение своевременной установкой критических обновлений, обеспечивающих безопасность системы), в других ситуациях они могут выявлять подозрительное поведение, например, при мониторинге активности других пользователей, имеющих доступ к той же сети.

### 4.2. ЧАСТНЫЙ СЕКТОР

Как уже упоминалось, частный сектор особенно уязвим к атакам с применением программ-вымогателей, особенно если компания пользуется устаревшим программным обеспечением или не соблюдает должный уровень «кибергигиены» в служебных ИТ-системах. Эта общая проблема касается практически всех компаний среднего размера, но некоторые секторы обнаруживают повышенную уязвимость к враждебным кибероперациям ввиду недостаточной готовности к работе в киберпространстве. Как отмечалось выше, эта проблема особенно актуальна для здравоохранения – сектора, где во многих странах ощущается недофинансирование в сфере кибербезопасности. Напротив, финансовый сектор обычно выделяет значительные средства на реализацию мер кибербезопасности и, подвергаясь частым кибератакам, достиг значительно более высокого уровня готовности к их отражению. К другим секторам с повышенной уязвимостью были отнесены фармацевтические и промышленные компании, где на производственных площадках нередко используется устаревшее оборудование. Замена таких старых станков и машин сопряжена с большими затратами, поэтому они продолжают эксплуатироваться долгое время после того, как были разработаны обновления безопасности для их операционных систем или систем управления. Эти уязвимости обычно хорошо известны потенциальным злоумышленникам. Даже в тех случаях, когда производственные участки работают в пределах внутренней сети в автономном режиме, т. е. без подключения к интернету, они остаются уязвимыми к хакерским атакам, особенно если служебная информация передается третьим лицам или если посторонние могут физически проникнуть на территорию предприятия.

<sup>13</sup> <https://www.cptomagazine.com/cyber-security/brazils-health-ministrys-website-data-leak-exposed-243-million-medical-records-for-more-than-6-months/>

Уязвимости также могут обнаруживаться в тех секторах, где быстрыми темпами шла цифровизация или внедрялись новые технологии, но не выделялись достаточные ресурсы на создание современных систем и политик кибербезопасности, включая межсетевые экраны или программы обнаружения несанкционированного доступа, которые могли бы защитить производственные активы. В подобных случаях слабые места в системах безопасности приходится устранять задним числом, что повышает вероятность сохранения скрытых уязвимостей.

Кроме того, повышенная уязвимость может порождаться рисками в цепочках поставок. Поставщики программного обеспечения часто не знают о наличии стороннего кода в их продуктах. Как следствие, отсутствует понимание потенциальных уязвимостей и, соответственно, возможность их должным образом устранить. Это в полной мере касается производственных процессов, когда компания-поставщик устанавливает систему, включающую компоненты нижнего уровня, которые могли быть скомпрометированы. Особенно актуальна данная проблема при использовании устройств интернета вещей, которые нередко выпускаются по минимальной стоимости, а это означает, что производители используют быстро устаревающее ПО без возможности его обновления (поскольку это потребовало бы дополнительных затрат), что делает устройства уязвимыми для хакеров.

Наконец, многие компании и объекты не располагают квалифицированным персоналом для внедрения мер кибербезопасности. Причиной может быть недостаточное финансирование организации, что, в частности, типично для предприятий водоснабжения и медицинских учреждений многих стран. Помимо этого, многие малые и средние предприятия не располагают достаточным бюджетом для найма специалистов по кибербезопасности. При этом многие вакансии остаются незакрытыми из-за дефицита квалифицированных и опытных кадров в этой сфере.

## 4.3. ГОССЕКТОР И КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА

Растущая уязвимость наблюдается и со стороны критической инфраструктуры, где идет процесс коммодитизации атак. В результате повсеместной приватизации, особенно в западных странах, многие операторы критической инфраструктуры более не относятся к государственному сектору. Повышенная уязвимость отчасти объясняется слиянием производственно-технологических (ПТ) и информационно-технологических (ИТ) сетей, например, в случаях, когда системы управления производственными процессами (СУПП) подключены к ИТ-сетям в целях дистанционного обслуживания. Число атак, нацеленных на СУПП и промышленное оборудование, растет быстрыми темпами.

Здесь также значимым фактором является растущая взаимосвязанность множества различных видов критической инфраструктуры – например, при подключении медицинского оборудования интернету; системы водоснабжения также неуклонно переходят на цифровое управление. Системы управления критической инфраструктурой особенно уязвимы (и потенциальные последствия могут проявиться даже на общенациональном уровне), когда они работают на одном и том же операционном ПО или программах для СУПП в разных секторах и у разных операторов (см. выше материал по рискам в цепочках поставок, раздел 2.3). Новейшие версии сложных вредоносных программ, в том числе вымогательских, способны автоматически определять тип взломанной СУПП, то есть такая программа «понимает», что она внедрилась, например, в систему, управляющую магистральной линией водопровода или электросетью. Это позволяет более точно нацеливать атаки и одновременно повышает уязвимость критической инфраструктуры, которая становится объектом «охоты по-крупному» (см. выше раздел 2.1).

На всем протяжении обсуждения подчеркивалось, что защита критической инфраструктуры остается в целом недостаточно изученной темой и что сам термин по-разному определяется в каждой стране или регионе. Региональные особенности существенным образом влияют на то, что именно признается «критическим». В этом контексте один из экспертов отмечал, что в

некоторых африканских странах, расположенных к югу от Сахары, ввиду отсутствия полноценной инфраструктуры наземных сетей связи мобильная связь играет гораздо более важную роль, чем другие ИТ-системы, в обеспечении социально значимыми услугами, включая микрофинансирование, оплата медицинских услуг или предоплата электроэнергии. Было также указано, что определенные секторы могут характеризоваться разной уязвимостью в зависимости от страны или региона. Хотя в странах Запада финансовый сектор в целом хорошо защищен от враждебных киберопераций, то же самое нельзя сказать о ряде стран Глобального Юга, где менее развиты стандарты кибербезопасности.

Вопрос о том, что составляет критическую инфраструктуру, крайне важен, поскольку от ответа на него может зависеть подход к ее защите. Кроме того, отнесение сектора к критической инфраструктуре и степень его подверженности риску меняется со временем и зависит от интересов атакующей стороны в каждом конкретном случае. В определенный момент времени тот или иной сектор может обрести особую ценность в силу действия внешних факторов и, как следствие, стать особенно уязвимым к враждебным действиям в киберпространстве.

Тенденции последнего времени, в том числе связанные с пандемией COVID-19, вновь показали, что сектор здравоохранения характеризуется повышенной уязвимостью, особенно учитывая ограниченность бюджетных средств, обычно выделяемых на цели кибербезопасности. Дополнительным фактором уязвимости являются ожидания, что в случае атаки с использованием программ-вымогателей органы, ответственные за медицинские учреждения, быстро заплатят выкуп, так как от этого могут зависеть человеческие жизни. Особо следует упомянуть все чаще практикуемое подключение к интернету критических медицинских приборов, таких как кардиостимуляторы или аппараты искусственной вентиляции легких, для дистанционного обслуживания. Это создает дополнительный уровень уязвимости, порождающий высокий риск причинения вреда как медицинским учреждениям, так и самим пациентам. Ряд экспертов прямо высказывали опасения, что операции, предпринятые против учреждений здравоохранения, могут впоследствии

привести к смертельному исходу для пациентов.

В качестве еще одной уязвимой категории часто называют системы водоснабжения, и некоторые эксперты считают это самой большой проблемой защиты критической инфраструктуры. В отличие от поставщиков электроэнергии, водоснабжающие организации имеют дело с «гиперлокальной» и децентрализованной инфраструктурой. В условиях низкой бюджетной обеспеченности инфраструктура водоснабжения часто оказывается одной из наименее защищенных отраслей.

Существует множество обособленных водоснабжающих компаний, каждая из которых обслуживает относительно небольшое число домохозяйств. Это означает, что в случае атаки на них пострадают лишь немногие домохозяйства, если только речь не идет о таких мегаполисах, как, например, Нью-Йорк или Токио, где инфраструктура водоснабжения часто напоминает инфраструктуру электросетей в том смысле, что они эксплуатируются консорциумом водоснабжающих организаций. В последнем случае враждебная кибероперация, затрагивающая одного поставщика, может оказать негативное воздействие на более многочисленную группу людей. Кроме того, разные инфраструктурные системы также взаимозависимы. В случае с системами водоснабжения это означает, что при отсутствии подачи электроэнергии большинство насосных станций перестают работать, что еще больше усиливает уязвимость. То же самое касается и других объектов критической инфраструктуры, даже если некоторые из них – в первую очередь медицинские учреждения – в соответствии с законом должны быть оснащены системами резервного электроснабжения для таких чрезвычайных ситуаций, как длящаяся кибероперация против электросети.

Даже если в результате кибероперации качество питьевой воды изменяется незначительно и это изменение не создает угрозу для здоровья, сам факт нарушения ее чистоты может оказать негативное психологическое воздействие на гражданское население – например, когда неопределенность последствий кибероперации против водоснабжающей компании побуждает власти издавать распоряжение, чтобы граждане кипятили любую воду перед употреблением. Помимо этого, водоснабжение может быть

прервано в результате аварий, поскольку транспортировка воды сопряжена с трудностями. В такой кризисной ситуации могут сразу возникнуть затруднения со снабжением населения питьевой водой, особенно с ее доставкой в удаленные районы.

Еще одна область, заслуживающая внимания в данном контексте – это транспорт и логистика. В процессе цифровизации, например, многие склады были преобразованы в «умные склады», функционирование которых в значительной мере зависит от ИТ-систем и работающей сетевой инфраструктуры, при этом стандарты кибербезопасности не всегда успевали отражать эти стремительные преобразования. Та же ситуация становится все более актуальной для крупных торговых портов как единых комплексов. Враждебные операции против таких объектов транспортного сектора – например, атаки с применением программ-вымогателей с шифрованием логистических данных или нарушением работы цифровых навигационных систем – могут иметь серьезные вторичные последствия, если затронуты цепочки поставок таких критически важных товаров, как лекарства или медицинские приборы.

Один из экспертов подчеркнул, что секторы, ранее не подвергавшиеся атакам, могут быть более уязвимы, чем имеющие опыт реагирования на различные киберинциденты. Это объясняется тем, что инциденты кибербезопасности, с которыми пришлось столкнуться компании или другим компаниям в том же секторе, в целом повышают их осведомленность и готовность направлять больше ресурсов на устранение уязвимостей и неуклонно повышают устойчивость к киберугрозам.

Еще один фактор уязвимости – зависимость от одной инфраструктурной системы или единственного поставщика. Примером может служить страна, которая ведет всю торговлю, например, медикаментами и медицинскими принадлежностями исключительно через один морской порт. В менее развитых странах секторы электроснабжения и водоснабжения характеризуются значительно меньшей диверсификацией, что ставит многих людей в зависимость от единственного поставщика и делает общество особенно уязвимым.

Однако растущее число наблюдаемых

киберопераций против критической инфраструктуры, в том числе систем водоснабжения, следует оценивать с осторожностью. На фоне повышенного внимания к данному вопросу возникает «искажающее влияние заметности» (англ. *“visibility bias”*). Кроме того, растущая взаимосвязанность элементов сделала сети более уязвимыми, а атаки – более успешными, но это не означает, что они не имели место до того, как системам водоснабжения стали уделять больше внимания.

#### 4.4. ОБЩЕСТВО

Уязвимость общества во многом зависит от уровня интеграции технологий, так как взаимосвязанность систем через интернет предполагает потенциально более разрушительные последствия киберопераций. Эта тенденция усиливается спросом общества на все новые цифровые возможности. Степень воздействия враждебных киберопераций прямо пропорциональна степени интеграции общественных процессов и жизни людей в цифровое пространство и зависит от того, насколько общество полагается на взаимосвязанные цифровые технологии. В этом отношении могут наблюдаться различия, связанные с демографической структурой общества; возрастной фактор в целом определяет зависимость от технологий. Вместе с тем, один из экспертов причислил самых молодых и самых пожилых членов общества к наиболее уязвимым категориям, учитывая ограниченную осведомленность этих возрастных групп в вопросах кибербезопасности, что делает их легкой добычей злоумышленников, прибегающих к фишингу или мошенническим схемам с банковскими онлайн-операциями.

Воздействие киберопераций на общество также зависит от их продолжительности и от сочетания с другими мерами. Кратковременное отключение подачи электроэнергии может иметь менее выраженный эффект, чем длительный период времени без электричества; кроме того, общество, привыкшее к перебоям в электроснабжении, меньше других уязвимо к таким атакам. Особенно высокому риску общество подвергается, если при отключении интернета пропаганда распространяется через текстовые сообщения. Это не просто дешевый способ связи, а метод распространения информации, который значительно ограничивает для граждан



возможность проверки ее достоверности с помощью интернет-ресурсов. Подобная ситуация может вызвать еще большее недоверие к государству и его институтам.

В целом гражданские организации и процессы представляют собой более легкую цель для военных киберопераций, чем вооруженные силы противника. Как упоминалось ранее, избирательные процессы являют собой особенно уязвимый объект атак, привлекательный для тех, кто ставит целью разжечь конфликт или изменить политический ландшафт и ситуацию в стране. В связи с этим ряд экспертов указали на то, что менее развитые страны могут быть более подвержены таким воздействиям, учитывая их в целом менее зрелые и менее устойчивые демократические системы. Информационные операции, рассчитанные на вмешательство в выборы, будут усугублять недоверие и скептицизм по отношению к демократическому процессу. Пропаганда и дезинформация могут также порождать напряженность между этническими и религиозными группами и в худшем случае даже приводить к вспышкам насилия на почве выборов.

Данный пример подчеркивает значимость того факта, что общества особенно уязвимы там, где сетевая взаимосвязанность достигла высокого уровня, и это касается не только западных стран, но и стран Глобального Юга, где может быть особенно выражена зависимость от определенных технологий, таких как службы текстовых сообщений или единственная социальная сеть, действующие как фактические монополии. Такая ситуация может привести к возникновению сбоев в критических точках и к другим системным рискам.<sup>14</sup> Одним из ярких примеров в этом контексте служит распространение дезинформации и риторики ненависти в сети Facebook в Мьянме.<sup>15</sup> Еще один пример, на который указали эксперты – Эфиопия, где, несмотря на относительно ограниченную интеграцию технологий в обществе,

искаженная информация, дезинформация и риторика ненависти усилили напряженность и привели к местным вспышкам насилия.<sup>16</sup>

Помимо сетевой взаимосвязанности существуют другие заслуживающие внимания внешние факторы, которые могут повысить уязвимость общества. По мнению одного из экспертов, чем дальше объект кибероперации находится от зоны конфликта и бедности, тем выше вероятность того, что (во всяком случае, по ситуации на сегодняшний день) ущерб сведется к нарушению в работе систем. Напротив, кибероперация, предпринятая, например, с целью помешать доставке гуманитарной помощи путем нарушения работы систем связи, может с большей вероятностью причинить физический вред.

<sup>14</sup> См. также ICRC, *Harmful information: Misinformation, disinformation and hate speech in armed conflict and other situations of violence* (Информация, несущая вред: искаженная информация, дезинформация и риторика ненависти в вооруженных конфликтах и в других ситуациях, связанных с насилием), ICRC, 2021, <https://www.icrc.org/en/publication/4556-harmful-information-misinformation-disinformation-and-hate-speech-armed-conflict>.

<sup>15</sup> См. Paul Mozur, A Genocide Incited on Facebook, with Posts from Myanmar's Military (Геноцид, разжигаемый в сети Facebook в публикациях военных Мьянмы) New York Times, 15 октября 2018 г., <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>.

<sup>16</sup> См. Peter Mwai, Ethiopia's Tigray Conflict Sparks Spread of Misinformation (Конфликт в эфиопской провинции Тыграй спровоцировал распространение искаженной информации), BBC, 11 ноября 2020 г., <https://www.bbc.com/news/world-africa-54888234>.

## СИТУАЦИОННЫЙ ПРИМЕР: COVID-19

Пандемия Covid-19 может служить хрестоматийным примером того, как целый ряд факторов, не связанных напрямую с проблемами кибербезопасности, в сочетании с меняющимся контекстом может повлиять на общественные риски и уязвимости в связи с враждебной киберактивностью.

Во-первых, в связи с продолжающейся всеобщей цифровизацией и, в частности, резким переходом многих сотрудников на удаленную работу пользователи и компании столкнулись с новыми угрозами. Прежде всего, практика удаленного подключения сотрудников, работающих на дому, к корпоративным сетям делает компании более уязвимыми, поскольку у многих из них отсутствуют протоколы с достаточным уровнем защиты их облачных сервисов. Другой потенциальной мишенью являются базовые маршрутизаторы ввиду заложенных в них, как правило, невысоких стандартов кибербезопасности, хотя эксперты пока не наблюдали роста числа атак на эти устройства. Кроме этого, физические лица стали объектами целенаправленных фишинговых кампаний, эксплуатирующих тематику Covid-19, и дезинформации. Они также подвергались атакам с применением программ-вымогателей, при этом злоумышленники задействовали уже существующие программы, но адаптировали их под тематику Covid-19.

Во-вторых, пандемия Covid-19 яснее показала степень уязвимости сектора здравоохранения. Еще до начала пандемии больницы и другие медицинские учреждения оказались подвержены враждебной киберактивности из-за традиционно скудных бюджетных средств, выделяемых на цели кибербезопасности, и, как следствие, в целом низкого уровня киберзащиты (см. выше раздел 4.3) по сравнению с другими секторами, включая финансовый. Больницы, работающие с предельной нагрузкой, стали особенно уязвимы к кибератакам, в частности, с использованием программ-вымогателей. Широко обсуждался инцидент, произошедший в университетской клинике Дюссельдорфа в сентябре 2020 г. В тот момент, когда компьютерная система клиники вышла из строя в результате вымогательской атаки, реанимационное отделение не смогло принять пациента, находящегося в критическом состоянии. Этот пациент умер по пути в другую больницу. И хотя позже в ходе расследования было отвергнуто предположение, что именно инцидент кибербезопасности привел к смерти пациента, эксперты почеркнули, что подобное может произойти в ближайшем будущем.

В-третьих, с начала пандемии наблюдался рост числа дезинформационных кампаний, связанных как с вирусом Covid-19 вообще, так и с вакцинами в частности. Например, широкое распространение получила ложная информация о том, что технология 5G распространяет вирусы. Противостоять подобным информационным кампаниям особенно трудно, так как их действие усиливается через социальные сети. Дополнительным фактором явился недостаток исследований и отсутствие научного консенсуса – во всяком случае, на ранних этапах пандемии – в вопросах, касающихся происхождения вируса, возможных методов лечения или эффективности мер на уровне системы здравоохранения.<sup>17</sup>

Помимо дезинформации о вакцинах, имели место кибероперации, нацеленные непосредственно на проекты разработки вакцин и государственные программы вакцинации, например, в форме «вакцинного шпионажа» против исследовательских центров и других организаций, занятых разработкой вакцин. Проводились также другие кибероперации, в частности, атаки с применением программ-вымогателей на компании, проводящие медицинские исследования.<sup>18</sup>

<sup>17</sup> См. US Gov: <https://www.cisa.gov/publication/covid-19-disinformation-activity>.

<sup>18</sup> См. M. Schmitt, 'Cyber Operations against Vaccine R & D: Key International Law Prohibitions and Obligations'

(Кибероперации против исследований и разработок в области вакцин: Ключевые положения международного права по запретам и обязательствам), *EJIL:Talk!*, 10 августа 2020 г., <https://www.ejiltalk.org/cyber-operations-against-vaccine-r-d-key-international-law-prohibitions-and-obligations/>.

## VI. УСТОЙЧИВОСТЬ

Степень воздействия киберопераций зависит не только от уязвимости объекта атаки, о чем шла речь в предыдущем разделе. Она напрямую связана с вопросами устойчивости: «Насколько готов потенциальный объект атаки предотвратить кибероперацию против своих систем?» или «Имеет ли компания, подвергшаяся вымогательской атаке, резервные копии своих данных, чтобы быстро восстановить работоспособность?». Для повышения устойчивости могут быть предприняты различные шаги, направленные на предотвращение ущерба от кибератак – в частности, введение усиленных мер кибергигиены или более тщательное исследование слабых мест в системе безопасности. В ситуациях, когда предпринимаются информационные операции против обществ, необходимы меры долгосрочного характера в области просвещения, чтобы общество могло лучше противостоять дезинформации. Ключевыми темами в этой связи также являются атрибуция (об эффективности которой в качестве сдерживающего фактора эксперты не сошлись во мнении) и восстановление (по мнению ряда экспертов, этой теме часто не уделяется должное внимание).

### 5.1. УПРЕЖДАЮЩИЕ МЕРЫ

#### МЕРЫ БЕЗОПАСНОСТИ И ЗАЩИТЫ

Для устранения потенциальных уязвимостей можно наметить два принципиальных шага: (1) адекватное признание существующей проблемы и (2) соответствующие инвестиции в ее решение. Необходимость упреждающих мер возрастает в свете того очевидного факта, что развитие возможностей для проведения наступательных операций в целом на годы опережает развитие защитных возможностей. Предотвращению киберопераций могут способствовать некоторые современные технологии, в частности, системы обнаружения вторжений на основе ИИ. Однако остается другая проблема: для правильного применения большинства технически сложных защитных мер необходим

соответствующим образом обученный персонал – этот важный ресурс у многих компаний, (потенциально) подвергающихся атакам, по-прежнему отсутствует. Даже лучшие инструменты не смогут эффективно предотвратить инциденты кибербезопасности, если их применяют неопытные или плохо подготовленные сотрудники.

Там, где речь идет об операциях с применением программ-вымогателей, упреждающие меры могут во многих случаях ограничить последствия таких атак – например, с помощью современных программных средств, позволяющих обнаруживать враждебные операции на этапе эксплуатации уязвимости, можно добиться прерывания этого процесса. Кроме того, можно остановить шифрование данных, применив инструменты, способные по общим признакам выявить идущий процесс шифрования и не допустить модификацию исходных данных.

Что касается предупреждения рисков в цепочках поставок, были высказаны рекомендации производителям снабжать своих заказчиков, пользователей и экосистему разработки дополнительной информацией и инструментами, которые позволят им понять текущие и будущие угрозы, чтобы лучше защититься от них. Поставщикам также следует обеспечить защиту своих заказчиков и пользователей, конструируя, разрабатывая и поставляя продукты и услуги, в которых приоритетом является безопасность, конфиденциальность, целостность и надежность. Это, в свою очередь, снизит вероятность и частоту появления уязвимостей, уменьшит возможность и критичность их эксплуатации, в значительной мере позволит избежать атак на цепочки поставок.

Другие долгосрочные меры, которые следует рассмотреть для повышения уровня безопасности, включают соблюдение тщательно продуманных правил кибергигиены. Это практичная мера, успех которой требует, в качестве первого шага, достижения общего понимания существующих проблем в сфере кибербезопасности. Помимо прочего, это предполагает отказ от использования устаревшего программного обеспечения, чтобы избежать так называемой проблемы унаследованных систем. Важно отметить, что практическая реализация принятой политики безусловно

имеет принципиальное значение для повышения уровня кибербезопасности. В этой связи некоторые эксперты критически оценивают тот факт, что слишком часто усилия сосредотачиваются на детальной разработке политики кибербезопасности, но при этом недостаточно внимания уделяется важнейшему следующему этапу – ее эффективной практической реализации.

Важным шагом к повышению общего уровня кибербезопасности является установление более тесного сотрудничества между государственными учреждениями и частными компаниями, например, в целях обмена информацией по кибербезопасности. В этом отношении любой эффективный анализ собранных данных о киберугрозах должен происходить на глобальном уровне и всегда учитывать позиции как государственного, так и частного сектора. Только при сотрудничестве всех секторов и взаимном информировании об угрозах, наблюдавшихся в их системах, другие субъекты могут более тщательно подготовить свои средства защиты, тем самым повысив устойчивость к будущим атакам. Однако такое сотрудничество требует взаимного доверия участников. В некоторых странах, включая Швейцарию, в этом отношении достигнуты большие успехи, тогда как другие страны пока отстают. Один из экспертов даже предложил создать международный механизм защиты от киберугроз, чтобы предотвращать злонамеренные действия против критической инфраструктуры на глобальном уровне.

В контексте защиты и устойчивости критической инфраструктуры один из экспертов обратил внимание на принципиальное различие понятий «защищенность» (англ. “security”) и «безопасность» (англ. “safety”). Даже если поставщики критической инфраструктуры не всегда обеспечивают должный уровень защищенности от кибератак, имея в виду, что злоумышленники имеют возможность проводить против них успешные кибероперации, это не обязательно означает, что физические активы или даже физические лица оказываются под угрозой. Как правило, существующие протоколы обеспечения безопасности на наиболее критических объектах (например, на водоочистительных станциях) обязывают персонал следить за их исправной работой

(например, контролировать качество питьевой воды), не полагаясь исключительно на ИТ-системы. Этот дополнительный уровень безопасности, действующий независимо от мер кибербезопасности, имеет прямое отношение к решению вопросов устойчивости и противостояния киберугрозам.

## **МЕРЫ ПО СНИЖЕНИЮ УЯЗВИМОСТИ К ДЕЗИНФОРМАЦИИ**

Одна из часто упоминаемых стратегий, призванных снизить уязвимость населения к дезинформации, состоит в наращивании усилий по обучению цифровой грамотности. Положительные результаты в этом отношении уже наблюдаются в ряде стран Балтии и Скандинавии, где школьников учат критически воспринимать новую информацию, проверять источники и анализировать качество информации.<sup>19</sup> В более общем плане особая значимость придается выявлению и распознаванию как ложного или вводящего в заблуждение контента, так и злонамеренных распространителей дезинформации. Некоторые эксперты дополнительно подчеркивали критическую важность разработки контрнарративов для отражения воздействия согласованных враждебных кампаний по дезинформации.

## **ГОТОВНОСТЬ НА УРОВНЕ ОБЩЕСТВА**

Важно особо отметить готовность всего общества к ситуациям, когда происходят серьезные инциденты кибербезопасности. Эту готовность можно повысить, обучая население действиям в случае, если кибероперации приведут к масштабным последствиям – например, к отключению всех каналов связи. Эта работа может вестись в форме, аналогичной гражданским учениям по отработке действий на случай землетрясения. Опыт подготовки всего общества в рамках общенациональной стратегии можно изучать на примере Швеции,

<sup>19</sup> См., напр., Maarit Jaakkola, Media literacy in the Baltics: Different approaches in neighbouring countries (*Медийная грамотность в странах Балтии: Разные подходы соседних стран*), Media & Learning, декабрь 2020 г., <https://media-and-learning.eu/type/featured-articles/media-literacy-in-the-baltics-similar-backgrounds-but-different-approaches/>.



где правительство разослало всем жителям страны информационные брошюры. В них разъяснялось, что в случае необходимости устранения последствий кибератаки, вызвавшей полное отключение цифровых каналов, вся связь будет переведена на радиоканалы, с рекомендацией включать автомобильные магнитолы при перебоях с электроснабжением.<sup>20</sup> Однако такая модель может оказаться не столь эффективной в более населенных странах или в обществах, характеризующихся меньшей степенью социальной сплоченности.

## 5.2. АТРИБУЦИЯ

Хотя в целом за последнее десятилетие возможности атрибуции враждебных киберопераций были усовершенствованы, установление субъекта кибератаки часто оказывается трудной задачей и требует больших временных затрат. Однако атрибуция имеет решающее значение в силу ряда причин, и прежде всего потому, что, устраняя возможности для правдоподобного отрицания причастности, может служить сдерживающим фактором для будущих организаторов атак. Кроме того, в процессе атрибуции нередко вскрываются значимые факты, касающиеся средств и методов ведения враждебных киберопераций. Впоследствии эта информация может быть использована для разработки технических механизмов защиты. Тем не менее, стало также очевидно, что атрибуция не обязательно является одной из главных задач каждого атакованного субъекта.

Некоторые эксперты подчеркивали, что атрибуция как таковая не всегда нужна для выработки эффективной практики кибербезопасности, во всяком случае, когда речь идет о производственном секторе, поскольку своевременное устранение слабых мест критичнее, но не требует атрибуции. Она, разумеется, более актуальна, когда решаются политические

задачи или предпринимаются шаги возмездия, например, в виде наложения санкций.

Атрибуция бывает затруднена, когда субъекты пытаются скрыть свои следы, проводя операции «под чужим флагом». Определить, задействована ли в операции маскирующаяся под кого-либо третья сторона, или операция действительно осуществлена предполагаемым субъектом или государством – сложная задача. Эта проблема особенно актуальна в случае программного взлома, так как сама вредоносная программа часто является единственной уликой, оставленной злоумышленниками. Учитывая тенденцию к проведению операций «под чужим флагом», часто невозможно с уверенностью отнести операцию к действиям того ли иного субъекта только на основе самого программного кода. Поэтому, наряду с юридически значимыми уликами, должны приниматься во внимание политические мотивы и стратегические интересы.

Вопрос о том, решает ли атрибуция на самом деле задачу сдерживания, вызвал дискуссию среди экспертов. По мнению некоторых, это прежде всего зависит от категории субъекта. Физические лица могут столкнуться с правовыми последствиями, и потому их может сдерживать перспектива быть обнаруженными в ходе кибероперации. Но едва ли то же можно сказать о национальных государствах, которым часто удается сохранить некоторую степень правдоподобного отрицания, даже при наличии против них веских улик. Однако некоторые эксперты полагают, что более частая и публичная атрибуция злонамеренных киберопераций может в конечном итоге произвести сдерживающий эффект.

Другие эксперты высказывались в целом более оптимистично, подчеркивая, что правоохранительным органам удастся выявлять тех, кто проводит кибероперации, и привлекать физических лиц к ответственности. В этой связи приводится пример операции «Ladybird», совместно осуществленной полицейскими органами нескольких стран для ликвидации вредоносной программы «Emotet», выросшей в целую сеть многочисленных ботнетов, которые предпринимали атаки для

<sup>20</sup> Swedish Civil Contingencies Agency, If Crisis or War Comes (Шведское агентство по гражданским чрезвычайным ситуациям, «Если наступит кризис или начнется война»), май 2018 г., <https://www.documentcloud.org/documents/4481608-Om-Krisen-Eller-Kriget-Kommer-Engelska.html#document/p1>.

получения выкупа и кражи данных.<sup>21</sup> Сами киберпреступники все яснее осознают свой риск, что проявляется во все более изощренных мерах защиты, с помощью которых они пытаются уберечь свои системы от обнаружения.

Наконец, общей проблемой атрибуции является достоверность заявлений о ее результатах; достоверность в значительной мере зависит от субъекта, делающего подобное заявление. Чтобы утверждения о злонамеренных действиях в киберпространстве были более убедительны для общественности, один из экспертов предложил создать нейтральный международный механизм для установления фактов, устранения сомнений в атрибуции киберопераций и выявления тех, кто несет ответственность за злонамеренные действия. Однако было признано, что создать подобный механизм будет непросто в сложившейся геополитической ситуации.<sup>22</sup>

### 5.3. ВОССТАНОВЛЕНИЕ

Негативное воздействие кибероперации существенно возрастает при несвоевременной реакции и медленном восстановлении. Это особенно справедливо в отношении инцидентов, цель которых – подорвать доверие населения к государственным институтам, но то же самое касается предприятий малого и среднего бизнеса, которые часто испытывают трудности с восстановлением после инцидентов кибербезопасности. Когда компания подвергается вымогательской атаке, встает вопрос: стоит ли платить выкуп, чтобы получить ключ для дешифровки файлов? Проблема в том, что успех такого обмена не гарантирован. Кроме того, хакер может снова проникнуть в систему через ту же брешь и повторно потребовать от компании выкуп. Эксперты в

целом были единодушны в том, что поэтому платить выкуп нежелательно. Более того, недавно в теневом сегменте интернета циркулировал список компаний, которые будут готовы заплатить, а это значит, что заплатившая компания подвергается риску многократных атак с применением вымогательских программ. Более приемлемая альтернатива для жертвы атаки – не платить выкуп, а постараться найти брешь и закрыть ее, чтобы повысить уровень кибербезопасности и в дальнейшем восстановить свои системы.

Жертвы примитивных вымогательских атак также имеют шанс ускорить восстановление, произведя дешифровку своих данных с помощью бесплатных программ-декрипторов. Самое главное – регулярно осуществлять резервное копирование данных, это позволит ускорить процесс восстановления благодаря доступу к исходным данным. Актуальной остается и задача выявления и ликвидации уязвимостей, через которые злоумышленники получили доступ в систему компании. Дополнительные шаги, способствующие восстановлению и помогающие компании сохранить репутацию и доверие потребителей – продуманная публичная реакция и обращение в суд. В связи с этим один из экспертов высказал мнение, что компания, подвергшаяся вымогательской атаке, может улучшить свое положение, с самого начала открыто признав факт такой атаки.

Поскольку восстановление после различного рода кибератак сопряжено с трудностями, значительно выросло число страховых продуктов с покрытием риска кибератак. В некоторых случаях страховая компания может брать на себя уплату выкупа. Такая практика рядом экспертов оценивается критически, поскольку может побудить застрахованную компанию менее тщательно подходить к вопросам кибергигиены, зная, что страховщик придет на помощь в случае инцидента. К тому же в случае выплаты выкупа по страховке лицо, предпринявшее атаку, может получить стимул к повторению своего преступления. Однако так бывает не всегда: после того, как кибероперация с применением вируса «NotPetya» вывела из строя ИТ-системы сразу многих компаний, их страховщики отказались покрывать убытки, сославшись

<sup>21</sup> См. Andy Greenberg, Cops Disrupt Emotet, the Internet's 'Most Dangerous Malware' (*Полицейские пресекли деятельность Emotet, «самого опасного вредоноса» в интернете*) Wired, 27 января 2021 г., <https://www.wired.com/story/emotet-botnet-takedown/>.

<sup>22</sup> См. также Yuval Shany and Michael N. Schmitt, An International Attribution Mechanism for Hostile Cyber Operations (*Международный механизм атрибуции враждебных киберопераций*), *International Law Studies*, Выпуск. 96, 2020, стр. 196–222.

на то, что эта операция, которую западные страны приписывали России и которая, как утверждалось, имела место в контексте более крупного конфликта между Россией и Украиной,<sup>23</sup> должна была характеризоваться как «военные действия», что по условиям договора исключает страховую выплату.<sup>24</sup> В техническом отношении ценность страхования также оценивается с осторожностью – ряд экспертов выразили сомнение в том, что наличие страховки улучшает ситуацию с кибербезопасностью. Напротив, они полагают, что наличие страховой защиты может побуждать компании идти на дополнительный риск. Со своей стороны, киберпреступники могут быть заинтересованы выбирать в качестве объектов атак именно застрахованные компании, так как они с большей вероятностью будут готовы платить. Однако в тех случаях, когда страховые продукты предусматривают стимулы, например, в виде сниженных премий, для соблюдения эффективных мер кибергигиены, страхование действительно может быть признано полезным инструментом.

## VII. ВЫВОДЫ О ПРИМЕНИМЫХ НОРМАХ ПРАВА

Сложившийся и быстро меняющийся ландшафт глобальных киберугроз, охарактеризованных экспертами-участниками семинаров, позволяет сделать ряд выводов, относящихся к разным областям права. Некоторые из этих аспектов были кратко затронуты в ходе семинаров. Вместо всеобъемлющего заключения по итогам экспертных консультаций в этом разделе будут освещены темы и аспекты, требующие дальнейшего вовлечения правоведов и лиц, принимающих политические решения.

<sup>23</sup> См., напр., United States, Statement from the Press Secretary (США, заявление пресс-секретаря), 15 февраля 2018 г., <https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/>; Australian Government Attribution of the “NotPetya” Cyber Incident to Russia (Правительство Австралии возлагает на Россию ответственность за киберинцидент с вирусом “NotPetya”), 16 февраля 2018 г., <https://www.dfat.gov.au/sites/default/files/australia-attribution-notpetya-malware-to-russia.pdf>.

Во-первых, говоря о стремительном росте числа инструментов для кибератак, можно рассматривать некий механизм, регулирующий распространение и использование государствами, по крайней мере, тех видов вредоносных программ, которые представляют наибольшую потенциальную опасность для отдельных граждан и гражданского населения. В качестве примера можно назвать самораспространяющиеся вредоносные программы, наносящие урон в равной мере гражданским и военным объектам, по определению относящиеся к средствам неизбирательного действия и потому запрещенные к применению во время вооруженных конфликтов. Однако участники положительно оценили возможное введение обязательного требования о том, чтобы вредоносный код был способен проводить такое различие. Некоторые эксперты подчеркивали, что существует техническая возможность написать вредоносный код таким образом, чтобы даже при автономном распространении от системы к системе заложенные в него инструкции исполнялись только при проникновении в заранее заданный объект воздействия. Один эксперт отметил, что компьютерный червь Stuxnet уже был спроектирован с расчетом на такое точное и избирательное действие, и даже если им были заражены тысячи ИТ-систем в разных странах, он наносил урон только иранским установкам по обогащению урана – как и было задумано, по заявлению его создателей.<sup>25</sup> Помимо решения серьезной проблемы контроля за соблюдением, государствам, разрабатывающим или приобретающим кибероружие, следует рассмотреть введение норм об обязательном наличии такой функции различения целей – за пределами более узкого контекста, в котором действует принцип различения целей в международном гуманитарном праве.

<sup>24</sup> См., напр., Adam Satariano & Nicole Perlroth, Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong (Крупные компании думали, что страховка покрывает кибератаки. Возможно, они ошибаются.), New York Times, 15 апреля 2019 г., <https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html>.

<sup>25</sup> См. P.W. Singer, Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons (Stuxnet и его скрытые уроки по этике кибероружия) (2015) 47 Case Western Reserve Journal of International Law 79, 85.

Вторая тематическая область касается вопросов информационных операций и шпионажа. Обсуждая первый из этих аспектов, эксперты были единодушны в том, что проблема использования в борьбе с противником ложной или вводящей в заблуждение информации, ориентированной на население других стран, приобретает все большую остроту и будет иметь долгосрочные, далеко идущие последствия. При этом они в целом скептически оценили перспективы эффективного пресечения такой деятельности (международно-)правовыми средствами, учитывая сложности с определением этой деятельности, оценкой и измерением причиненного ущерба. Что касается шпионажа, эксперты усомнились в том, что традиционная парадигма действующего международного права (в рамках которого данная практика не является ни разрешенной, ни запрещенной) является удовлетворительной в свете потенциальных негативных последствий повсеместной слежки в интернете или методов разведки, направленных на «подготовку боевых действий».

Наконец, были подняты вопросы о

будущей роли невоенных субъектов во время киберконфликтов. Поскольку инфраструктура базовых сетей в основном находится в руках частных компаний, такие компании могут иметь возможность – или даже быть обязаны – подавлять злонамеренную активность, при этом на стороны вооруженного конфликта также могут налагаться жесткие обязательства не наносить ущерб такой инфраструктуре, учитывая потенциальные негативные последствия для глобальных сетей, от которых зависит современное общество. В ходе консультаций была отмечена параллельная тенденция – растущая вовлеченность служб гражданской разведки в военные кибероперации. С точки зрения международного гуманитарного права, участие гражданских субъектов – как частных, так и государственных – в решении задач, традиционно ассоциируемых с государственными вооруженными силами, ставит вопрос о том, следует ли – и в каких случаях – расценивать это как прямое участие в военных действиях, что влечет утрату права на защиту для соответствующих лиц.



# ПРИЛОЖЕНИЕ 1: СПИСОК ЭКСПЕРТОВ

## ПРИГЛАШЕННЫЕ ЭКСПЕРТЫ

Г-н Бенджамин Анг, Центр передового опыта по вопросам национальной безопасности, Наньянский технологический университет, Сингапур  
Г-н Лиор Бар-Лев, Независимый эксперт по киберустойчивости, Израиль  
Г-н Бернхардс Блумбергс, CERT.LV, Латвия  
Г-н Серджио Калтаджироне, Разведка киберугроз, Dragos, США  
Г-н Джейсон Хили, Школа международных и общественных отношений Колумбийского университета, США  
Г-н Барт Хогевен, Международный центр киберполитики, Австралийский институт стратегической политики, Австралия  
Г-н Релто Инверсини, Группа реагирования на компьютерные чрезвычайные ситуации правительства Швейцарии  
Г-н Виталий Камлюк, Касперский, Сингапур  
Г-н Макс ван Кралинген, Отдел ИТ-безопасности и управления риском, Merck & Co., США  
Г-жа Марина Кротофил, ISSP - Information Systems Security Partners, Великобритания  
Г-жа Тан Лань, Китайский институт современных международных отношений, Китай  
Г-н Юэн Лоусон, Королевский объединенный институт оборонных исследований (RUSI), Великобритания  
Д-р Херб Лин, Центр международной безопасности и сотрудничества Стэнфордского университета, США  
Г-н Сюй Лонгди, Китайский институт международных исследований, Китай  
Д-р Ангелос Марнеридес, Университет Глазго, Великобритания  
Проф. Киаран Мартин, Оксфордский университет, Великобритания  
Г-жа Михоко Матсубара, NTT Corporation, Япония  
Д-р Мари Мо, Фонд научных и промышленных исследований (SINTEF) и Норвежский университет естественных и технических наук (NTNU), Норвегия  
Г-жа Фолаке Олагунжу Ойелола, ЭКОВАС  
Г-н Лукаш Олейник, Независимый консультант и исследователь по вопросам безопасности и конфиденциальности, Бельгия и Великобритания  
Г-жа Арина Пазушко, VI.ZONE, Россия  
Проф. Адриан Перриг, Федеральный технологический институт Цюриха, Швейцария  
Г-н Джакомо Паоли, ЮНИДИП  
Г-жа Корали Ромет, Институт Кибермира, Швейцария  
Г-н Томслин Самме-Нлар, ICANN, Камерун  
Г-н Матиас Шульце, Немецкий институт международных отношений и безопасности, Берлин, Германия  
Д-р Хайя Шульман, Институт безопасных информационных технологий Фраунгофера, Германия  
Г-жа Ева Телецка, Директор Отдела ИТ-безопасности и управления риском, Merck, Чешская Республика  
Г-жа Нозль ван дер Вагг-Коулинг, Институт безопасности управления и лидерства в Африке, Стеллонбошский университет, ЮАР  
Г-н Бен Вагнер, ТУ Дельфт, Факультет технологии, политики и управления, Австрия

## ЖЕНЕВСКАЯ АКАДЕМИЯ

Проф. Робин Гайсс, Директор ЮНИДИП

Д-р Хеннинг Ламанн, Международный научный сотрудник, Нью-Йоркский университет

Д-р Кьяра Рэделли, Научный сотрудник, Женевская академия международного гуманитарного права и прав человека

## МЕЖДУНАРОДНЫЙ КОМИТЕТ КРАСНОГО КРЕСТА

Г-н Бенджамин Шарлье, Советник по правовым вопросам, Подразделение по вопросам вооружений и ведения вооруженных конфликтов

Д-р Нил Дэвисон, Советник по вопросам науки и политики, Подразделение по вопросам вооружений и ведения вооруженных конфликтов

Г-н Лорен Жизель, руководитель Подразделения по вопросам вооружений и ведения вооруженных конфликтов

Д-р Кубо Мачак, Советник по правовым вопросам, Подразделение по вопросам вооружений и ведения вооруженных конфликтов

Д-р Тильман Роденхойзер, Советник по правовым вопросам, Подразделение по вопросам вооружений и ведения вооруженных конфликтов

Г-жа Дельфина ван Золинге, Советник по вопросам цифровых угроз, Отдел защиты

Г-н Рубен Стюарт, Советник по работе с вооруженными силами и вооруженными группами, Подразделение по взаимодействию с вооруженными силами и правоохранительными органами

## ПРИЛОЖЕНИЕ 2: УСТАНОВОЧНЫЕ ВОПРОСЫ

### I. ПОТЕНЦИАЛЬНЫЕ ГУМАНИТАРНЫЕ ПОСЛЕДСТВИЯ КИБЕРОПЕРАЦИЙ: ТЕНДЕНЦИИ ПОСЛЕДНЕГО ВРЕМЕНИ

*Эти вопросы составлены для анализа происходившей в последнее время эволюции киберопераций, а также для обновления углубленного анализа потенциальных гуманитарных последствий киберопераций, который МККК проводил ранее.*

1. Каковы тенденции происходившей в последнее время эволюции средств эксплуатации уязвимостей и вредоносных программ? Как изменилась ситуация за последние несколько лет с точки зрения видов операций и применяемых инструментов (напр., создаются специально под конкретные операции или универсальны по своим свойствам), вовлеченных в эту деятельность субъектов, обстоятельств, баланса средств нападения и защиты? Возрастают ли риски разрушительных киберопераций (более многочисленные или новые атакующие субъекты, больше возможностей), или они уменьшаются (больше ресурсов на цели кибербезопасности, выше уровень безопасности, более устойчивые системы), и как эти недавние изменения влияют на перспективную оценку будущих угроз?

2. Ситуация по отдельным секторам:

а. Каковы последние тенденции в изменении рисков, которым в результате кибератак подвергается сектор здравоохранения? В частности, как продолжающаяся пандемия COVID-19 повлияла на уязвимость и/или устойчивость сектора здравоохранения к вредоносному воздействию кибератак?

б. Каковы последние тенденции в изменении рисков, которым в результате кибератак подвергается критическая гражданская инфраструктура (кроме здравоохранения), в особенности имея в виду кибератаки, целью которых стали, или от которых пострадали, объекты энергетики, водоснабжения, транспорта или логистики, плотины, атомные электростанции, предприятия химической и биологической промышленности?

с. Каковы последние тенденции в изменении рисков, которым в результате кибератак подвергается базовые интернет-службы, включая Точки обмена трафиком (IXP), Служба доменных имен (DNS) или Центры сертификации (CA)? В частности, насколько устойчивы различные компоненты ядра интернета, и каков риск того, что кибератаки, нацеленные на эти компоненты, будут иметь серьезные негативные последствия?

### II. ОБЩЕСТВЕННЫЕ РИСКИ, ПОРОЖДАЕМЫЕ КИБЕРОПЕРАЦИЯМИ

*Цель этих вопросов – расширить рамки анализа, включив в него другие риски, которым подвергаются общества вследствие киберопераций, в том числе риск нарушения функционирования государственных служб, сферы финансовых услуг, экономики, систем связи, образовательных учреждений, риск в отношении других критически важных данных в гражданской сфере, а также риски, порождаемые информационными операциями.*

3. Что вызывает наибольшие опасения с точки зрения риска причинения вреда людям и обществам в результате киберопераций (наиболее неблагоприятный сценарий, тип риска, обстоятельства и цель применения, вероятность и тяжесть негативных последствий)?

4. Являются ли некоторые общества относительно более уязвимыми к определенным видам киберопераций? Какие факторы играют при этом роль (технологические, культурные, политические)?

5. Какие секторы общества особенно уязвимы к враждебным кибероперациям? Приведет ли вмешательство в определенные (критические) инфраструктуры / секторы общества к возникновению потенциальных системных рисков на уровне всего общества? Какие элементы киберпространства имеют такую значимость с системной/общественной точки зрения, что вмешательство в них ни в коем случае нельзя допустить, и как отличить их от прочих элементов?

6. Как цифровые технологии меняют/влияют на характер применения Государствами и другими субъектами информационных операций (таких как пропаганда, искаженная информация и дезинформация, риторика ненависти)? Какой риск создают такие операции для людей и обществ?

7. Каким образом можно сформировать надежный подход к измерению воздействия киберопераций на общество? Каковы критерии?

### III. ВОЕННЫЕ КИБЕРОПЕРАЦИИ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ

*Цель этих вопросов – дополнить анализ, обращаясь к ситуациям вооруженных конфликтов, в том числе проанализировав, в какой мере кибероперации, их применение и их последствия для гражданского населения или общества могут отличаться в мирное время и во время вооруженных конфликтов.*

8. Каких изменений вы ожидаете в разработке и применении военного киберпотенциала в среднесрочной и долгосрочной перспективе?

9. Какие могут наблюдаться различия при проведении враждебных киберопераций в мирное время и во время вооруженных конфликтов? В частности, каковы будут различия с точки зрения целей таких операций (напр., получение доступа, создание эффектов и т. п.), характера их применения (напр., число, вероятность и т. п.) и последствий для гражданского населения и для общества (напр., вид и тяжесть последствий, вероятность наступления вредных последствий) в ситуациях мира и вооруженного конфликта?

10. Какие стратегические и оперативные задачи будут стремиться решить Государства/вооруженные субъекты в киберпространстве и с помощью киберсредств во время вооруженного конфликта? Что значит стремиться к достижению превосходства в киберпространстве (с технической точки зрения, с точки зрения сопутствующих рисков и т. д.)? Что значит добиться превосходства в киберпространстве или доминировать в нем?

11. Как могут выглядеть кибервойны (понимаемые в рамках данного обсуждения как длительное военное противостояние хорошо подготовленных субъектов в киберпространстве) в обозримом будущем? Какие различия будут проявляться в таких противостояниях между ситуациями симметричными (включая так называемые конфликты с практически равным противником) и асимметричными (когда кибердержаве противостоит в конфликте менее развитое Государство или негосударственная вооруженная группировка)?

### IV. ПРОЧИЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ

12. Есть ли какие-либо важные аспекты, относящиеся к тематике семинара, которые не отражены в вышеизложенных вопросах или вообще не затрагиваются в современных дискуссиях? Есть ли какие-либо возможные эффекты, которые заслуживают более детального обсуждения? Возникают ли вследствие использования киберпространства и киберопераций специфические риски и потребности в защите, которые упускаются из виду в современных дискуссиях и должны быть освещены?





## ПРИЛОЖЕНИЕ 3: СПРАВОЧНЫЙ ДОКУМЕНТ

Проект «Цифровизация конфликта: Гуманитарные последствия и правовая защита» - совместная инициатива Международного комитета Красного Креста и Швейцарской кафедры МГП Женевской академии международного гуманитарного права и прав человека. Его задача - исследовать гуманитарные последствия и потребности в защите, возникающие вследствие цифровизации вооруженных конфликтов, а также определить степень, в которой эти потребности покрываются нормами международного права, в особенности международного гуманитарного права (МГП).

Цифровизация вооруженного конфликта – это динамический процесс, который заключается во все более активном применении цифровых средств и способов ведения войны, созданных на основе быстро эволюционирующих технологических разработок, прежде всего в сфере компьютерных и других цифровых технологий, искусственного интеллекта, машинного обучения, сенсорных систем и робототехники. Проект призван изучить последствия этих процессов – как по отдельности, так и в сочетании – с целью оценить риски, которые они порождают для затронутого конфликтом населения, и добиться того, чтобы нормативно-правовая база обеспечивала соответствующую гуманитарную защиту в современных и будущих войнах. Текущий первый этап проекта затрагивает вопросы, связанные с кибертехнологиями в военном контексте.

Новые технологии оказывают глубокое воздействие на характер ведения войн. Действие МГП распространяется на все технологические новшества, применяемые в военных целях. Однако темпы, масштабы и преобразующее воздействие выдающихся технологических достижений современности и продолжающееся сращивание физических и цифровых возможностей – все это требует постоянного (пере)осмысления новых средств и способов ведения войны для ответа на вопрос: соответствуют ли они действующим нормам МГП, и по-прежнему ли МГП обеспечивает тот уровень гуманитарной защиты, который оно призвано обеспечивать во время вооруженного конфликта?

Эта совместная инициатива базируется на мультидисциплинарном подходе, в котором рассматриваются взаимосвязанные технические, военные, этические, политические, правовые и гуманитарные аспекты для ответа на три всеобъемлющих вопроса:

1. Какие риски, потенциальные гуманитарные последствия и потребности в защите затронутого конфликтом населения возникают при ведении войн в цифровом пространстве?
2. Обеспечивают ли нормы международного права, в особенности МГП, эффективное снижение этих рисков и удовлетворение этих потребностей в защите?
3. Если нет, какие могут быть выработаны рекомендации в сфере права и политики за рамками действующих норм МГП для снижения этих рисков и обеспечения этих потребностей в защите?

В ходе семинара с тематическим фокусом на военном применении кибертехнологий эти вопросы будут рассматриваться в рамках консультаций с рядом выдающихся экспертов, обладающих компетенцией в различных теоретических и практических дисциплинах.

Общая цель семинара, открывающего серию мероприятий, состоит в том, чтобы дать актуальную оценку существующих рисков и потребностей в защите в свете современных военных кибервозможностей. Для этого семинар был разделен на три секции:

- (I) Потенциальные гуманитарные последствия киберопераций;
- (II) Общественные риски, порождаемые кибероперациями;
- (III) Военные кибероперации во время вооруженных конфликтов.

В качестве побуждения к дискуссии в настоящем справочном документе кратко излагается существенная информация по этим трем тематическим направлениям.

## I. ПОТЕНЦИАЛЬНЫЕ ГУМАНИТАРНЫЕ ПОСЛЕДСТВИЯ КИБЕРОПЕРАЦИЙ: ТЕНДЕНЦИИ ПОСЛЕДНЕГО ВРЕМЕНИ

В последние годы МККК углубил свою оценку рисков, порождаемых кибероперациями, и возможностей избежать непреднамеренного причинения вреда в военных кибероперациях. В частности, МККК провел глубокий анализ потенциальных гуманитарных последствий киберопераций, уделяя особое внимание риску того, что кибероперации могут привести к смерти, ранению или физическому ущербу, нарушить обеспечение населения критически важными услугами или затронуть базовые интернет-службы. Задача первой секции семинара – актуализировать и уточнить анализ и понимание потенциальных гуманитарных последствий киберопераций, особенно в свете технологических новшеств, появившихся с момента запуска первоначального исследования МККК.

Зависимость от цифровых информационно-коммуникационных технологий проявляется во многих аспектах жизни обществ, и начавшаяся пандемия COVID-19 лишь ускорила этот процесс. Это дает огромные преимущества и новые возможности, но с усилением зависимости растет и уязвимость. Хотя появление многочисленных киберсредств и их применение в качестве средств или способов ведения войны позволяет военным достигать своих целей, не обязательно причиняя прямой вред гражданскому населению или физический ущерб гражданской инфраструктуре, нельзя обходить вниманием потенциальные гуманитарные последствия киберопераций. Посредством таких операций процессы, управляемые компьютерными системами, могут быть запущены, изменены или подвергнуты иному внешнему воздействию. Характерная для киберпространства взаимосвязанность означает, что любой объект, подключенный к интернету, может стать целью кибероперации, запущенной из любой точки мира. Целенаправленная кибероперация против одной системы может создавать вторичные последствия для различных других систем, где бы они ни находились.

Существует реальный риск того, что киберсредства – намеренно или по ошибке – могут оказать масштабное и многоплановое воздействие на критическую гражданскую инфраструктуру, включая жизненно важные отрасли производства, электронную связь, транспорт, государственные и финансовые системы. Кибероперации, проведенные за последние несколько лет – в основном вне связи с вооруженными конфликтами – показали, что вредоносные программы могут распространяться мгновенно по всему миру, затрагивая гражданскую инфраструктуру и системы жизнеобеспечения.<sup>26</sup> По словам одного эксперта по кибербезопасности, такие военные операции – не что иное, как «назревающий гуманитарный кризис».<sup>27</sup>

Кибероперации могут повреждать инфраструктуру, как минимум, двумя способами. Во-первых, они могут нарушить процесс предоставления жизненно необходимых услуг гражданскому населению, как показали кибератаки на электросети и сектор здравоохранения. Во-вторых, они способны наносить физический ущерб, как в случае с атакой с помощью компьютерного червя Stuxnet на иранское предприятие по обогащению урана в 2010 г. и атакой на металлургический завод в Германии в 2014 г.

Особенно уязвимым стал сектор здравоохранения, где быстрыми темпами внедрялись цифровые технологии и системы, подключенные к интернету, без соответствующих усовершенствований в сфере кибербезопасности. В результате больницы и другие медицинские

Назначение этого справочного документа – предоставить актуальный материал и пищу для размышлений в поддержку дискуссии в ходе Встречи экспертов. Он не обязательно отражает взгляды или позиции Международного комитета Красного Креста.

<sup>26</sup> Среди примеров – вредоносная программа CrashOverride, программа-вымогатель WannaCry, программа-вайпер NotPetya и вредоносная программа Triton. CrashOverride нарушила подачу электроэнергии в Украине; WannaCry вмешалась в работу клиник в ряде стран; от вируса NotPetya пострадало большое число частных компаний; атака с применением Triton, имевшая целью повредить системы управления производственными процессами, как сообщалось, была предпринята против нефтехимических предприятий Саудовской Аравии. Частичное освещение этой темы см. в материале Laurent Gisel and Lukasz Olejnik, “The Potential Human Cost of Cyber Operations: Starting the Conversation” (*«Потенциальные гуманитарные последствия киберопераций: Начала диалога»*), *Humanitarian Law and Policy Blog*, 14 ноября 2018 г.

<sup>27</sup> Sergio Caltagirone, “Industrial Cyber Attacks: A Humanitarian Crisis in the Making” (*Промышленные кибератаки: назревающий гуманитарный кризис*), МККК, «Гуманитарное право и политика», 3 декабря 2019 г.

учреждения часто становятся целью злонамеренных операций, в особенности с началом пандемии. Кибероперации против других объектов критической гражданской инфраструктуры – сетей электроснабжения, водоснабжения и канализации – также могут причинить серьезный вред людям, оказывая физическое воздействие. Главная причина в том, что такая инфраструктура часто находится под контролем систем управления производственными процессами (СУПП), которые уязвимы к злонамеренным операциям в киберпространстве. Для проведения киберопераций против СУПП нужны особые знания и умения, а нередко и специально разработанные вредоносные программы. Хотя атаки на СУПП регистрируются реже других видов киберопераций, их частота, по имеющимся сведениям, неуклонно растет, и степень угрозы в последнее время возростала быстрее, чем предполагалось еще несколько лет назад.<sup>28</sup> Эксперты призвали международное сообщество специалистов по информационной безопасности, правительства стран и юристов, специализирующихся на гуманитарном праве, приступить к обсуждению путей регулирования таких киберфизических операций, поскольку они обладают потенциалом оказания кинетического воздействия и могут приводить к человеческим жертвам.<sup>29</sup>

Кроме того, особую озабоченность вызывают особенности самого киберпространства. Например, кибероперации несут в себе риск эскалации и связанного с этим причинения вреда людям по той простой причине, что атакованному субъекту бывает трудно определить, является ли целью злоумышленника сбор разведывательных данных («подрыв компьютерных сетей», CNE) или более вредоносное воздействие («атака на компьютерные сети», CNA). Жертва атаки может поэтому отреагировать на нее чрезмерно, ожидая, что реализуется наихудший сценарий. Средства кибернападения также развиваются уникальным образом. После первого использования они могут быть переориентированы на другую задачу или перепроектированы и, соответственно, могут найти широкое применение у других субъектов, нежели изначальный создатель или пользователь. Еще одна проблема – трудность с достоверной атрибуцией киберопераций. Это затрудняет обнаружение и привлечение к ответственности тех, кто нарушает международное право в киберпространстве. Представление о том, что будет проще отрицать свою причастность к подобным операциям, может также ослабить табу на их применение – а значит, такие субъекты будут свободнее прибегать к ним в нарушение международного права.<sup>30</sup>

Хотя на сегодняшний день кибероперации главным образом приводили к значительному экономическому ущербу, не причиняя серьезного вреда людям, многое остается неизвестным в отношении технологического развития, возможностей самых изощренных субъектов – включая военных – и разрабатываемых ими инструментов, а также в отношении того, насколько применение киберопераций во время вооруженных конфликтов может отличаться от наблюдаемых ныне тенденций. Иными словами, хотя риск гуманитарных последствий, исходя из текущих наблюдений, не представляется чрезвычайно высоким, особенно учитывая разрушения и страдания, к которым всегда приводят конфликты, эволюция киберопераций требует пристального внимания с учетом существующих факторов неопределенности и высоких темпов изменений.

## II. ОБЩЕСТВЕННЫЕ РИСКИ, ПОРОЖДАЕМЫЕ КИБЕРОПЕРАЦИЯМИ

*Этот раздел основан на двух готовящихся к выпуску рабочих документах Женевской академии: «Защита общества» и «Защита информационного пространства во время вооруженного конфликта».*

<sup>28</sup> Laurent Gisel and Lukasz Olejnik (eds), *ICRC Expert Meeting: The Potential Human Cost of Cyber Operations* (Экспертное совещание МККК: Потенциальные гуманитарные последствия киберопераций), ICRC, Geneva, 2019, стр. 25.

<sup>29</sup> Marina Krotofil, "Casualties Caused through Computer Network Attacks: The Potential Human Costs of Cyber Warfare", 42nd Round Table on Current Issues of International Humanitarian Law («Людские потери в результате компьютерных сетевых атак: Потенциальные гуманитарные последствия кибервойн», 42-й Круглый стол по современному проблемам международного гуманитарного права), 2019, стр. 8.

<sup>30</sup> ICRC, *International humanitarian law and the challenges of contemporary armed conflicts* (Международное гуманитарное право и вызовы современных вооруженных конфликтов), 2011, стр. 37; ICRC, *International humanitarian law and the challenges of contemporary armed conflicts* (Международное гуманитарное право и вызовы современных вооруженных конфликтов), 2019, стр. 20.



Действующие нормы МГП изначально задумывались с учетом принципиально иного характера военных действий. В целом их сфера применения и исходные предпосылки были ориентированы на физические последствия ведения военных действий и направлены на уменьшение страданий, причиняемых в результате физического насилия в его традиционном понимании. Поэтому представляется не вполне очевидным, что эти нормы могут эффективно регулировать весь спектр современных конфликтов, в которых задействованы киберсредства, и в достаточной мере сдерживать воюющие стороны.

Учитывая современные возможности ведения войн в киберпространстве, можно поставить вопрос о выходе на новый уровень понимания разрушительных последствий и вытекающих из них потребностей в защите. Это новое понимание связано с тем воздействием, которое военные кибероперации оказывают на функционирование жизненно важных общественных процессов в экономической, финансовой, научной, культурной и медицинской сферах, а также в связи с формированием общественного мнения и другими общественными функциями. Целью таких операций может быть парализация государственного управления по всей стране, кодирование данных налогового учета тысяч и миллионов граждан, нарушение работы коммунальных служб – водоснабжения, электроснабжения, удаления отходов – или масштабная дестабилизация финансовых рынков и цепочек поставок. Хотя эти факторы воздействия могут быть более разрозненными и неосязаемыми и труднее поддаются измерению, чем военные потери или физические разрушения, непосредственно вызванные кинетическими средствами ведения войны, в современном мире с неуклонно растущей взаимосвязанностью они могут затрагивать целые общества и приводить к системным сбоям. Если основываться на традиционном подходе, некоторые из этих факторов воздействия (в том числе экономический ущерб, не ассоциируемый с конкретными кибератаками, или психологические операции, не приравниваемые к запрещенным актам насилия или угрозе насилием с целью устрашения гражданского населения и не расцениваемые как подстрекательство к нарушениям МГП) были бы признаны не входящими в сферу регулирования МГП.

В этом смысле необходимо обсудить вопрос о том, можно ли рассматривать современный киберконфликт как смену парадигмы, учитывая, что серьезная и длительная дестабилизация гражданского общества все чаще становится реальностью в отсутствие какого-либо физического ущерба. Со временем эти новые тенденции могут начать восприниматься лишь как отправная точка в более фундаментальном изменении характера войны. В долгосрочной перспективе, в условиях стремительного развития технологий, постоянно растущей взаимозависимости и расширения «площади атаки» во всех сферах общества, возникает реальный риск постепенного подрыва – если не пересмотра – основополагающего принципа, согласно которому во время вооруженных конфликтов гражданское население не должно подвергаться нападению. С принятием узких толкований, которые ограничивают сферу применения норм МГП, касающихся ведения военных действий, физическими проявлениями насилия и ущерба, возникает риск, что ключевые аспекты гражданской жизни и существенные элементы гражданской инфраструктуры останутся без правовой защиты и будут подвержены прямым атакам в XXI веке.

В этой связи можно ставить вопрос о том, следует ли, исходя из особенностей ведения современной войны, выработать более комплексное понимание защиты гражданского населения; такое понимание будет учитывать принципиальную важность различных общественных процессов. Примечательно, что в сфере международного права мирного времени некоторые государства проявляют большую готовность дополнить правовые нормы новыми аспектами защиты, признающими включение нефизических воздействий на цифровые и на самые различные общественные процессы (экономические, финансовые, культурные) в сферу таких понятий, как суверенитет, невмешательство или применение силы. Принимая во внимание быструю эволюцию военного киберпотенциала и ресурсов, необходимо дальнейшее обсуждение этих вопросов в контексте МГП, а также в связи с экономическими, финансовыми и другими общественными процессами. При этом, что крайне важно, подразумевается не только гражданское население как таковое, т. е. физические лица с их физическим имуществом, непосредственно подвергающиеся риску причинения вреда, но и системные общественные процессы в широком понимании, нарушение которых повлечет серьезные последствия для всего

гражданского населения. Более того, некоторые государства и другие заинтересованные стороны высказывались в поддержку таких вариантов толкования, которые признавали бы допустимым применение масштабных операций против обществ во время вооруженных конфликтов.

Таким образом, предстоит решить непростую дилемму: следует ли, и в какой мере, усилить действующую правовую базу МГП, не расширяя чрезмерно сферу защиты этого правового режима, который, в силу своей природы, должен учитывать военную необходимость и военную реальность. Главный вопрос заключается в том, следует ли признать определенные общественные процессы и функции достаточно значимыми и жизненно необходимыми, чтобы распространить на них правовую защиту в соответствии с МГП во время вооруженного конфликта. В связи с этим семинар предусматривает обмен мнениями о том, обеспечивает ли МГП по состоянию на данный момент достаточную защиту различных сфер общественной жизни и общественных процессов, которые могут подвергнуться действию (тщательно подготовленных) киберопераций. Соответственно, мы ожидаем, что участники семинара поделятся имеющейся информацией и выскажут свои экспертные суждения о том, каким образом проведение киберопераций может отразиться на жизненно важных общественных процессах, помимо таких более очевидных и часто обсуждаемых последствий, как нарушение работы инфраструктуры.

### III. ВОЕННЫЕ КИБЕРОПЕРАЦИИ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ

*Этот раздел основан на готовящемся к выпуску докладе МККК и на материале статьи, недавно опубликованной в «Международном журнале Красного Креста» за авторством трех юристов МККК.*

Кибертехнологии стали реальностью современных вооруженных конфликтов и, по всей вероятности, будут находить все более широкое применение. Некоторые Государства открыто признают факты проведения киберопераций в текущих вооруженных конфликтах. В частности, США, Великобритания и Австралия раскрыли информацию, согласно которой они прибегали к кибероперациям, участвуя в конфликте против группировки «Исламское государство».<sup>31</sup> Существуют также открытые отчеты, из которых следует, что Израиль применял кибероперации против движения Хамас – и неподтвержденные заявления о том, что движение Хамас применяло кибероперации против Израиля.<sup>32</sup> Кроме того, кибероперации затронули другие страны, участвующие в вооруженных конфликтах, включая Грузию в 2008 г.,<sup>33</sup> Украину в 2015–17 гг.<sup>34</sup> и Саудовскую Аравию в 2017 г.,<sup>35</sup> хотя авторы этих киберопераций по сей день неизвестны, и атрибуция ответственности за них оспаривается. Следовательно, остается неясным, были ли эти операции связаны с

<sup>31</sup> См., в частности, Mike Burgess, Australian Signals Directorate, “Offensive Cyber and the People Who Do It”, speech given to the Lowy Institute (*«Наступательные киберсредства и люди, которые их применяют»*, речь, произнесенная в Институте Лоуи), 27 марта 2019 г.; Paul M. Nakasone, “Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services” (*«Доклад генерала Пола Накасоне, начальника Управления киберопераций США, в сенатском Комитете по делам вооруженных сил»*), 14 февраля 2019 г.; Jeremy Fleming, GCHQ, “Director’s Speech at CyberUK18,” (*«Выступление директора [Центра правительственной связи Великобритании] на конференции CyberUK18»*), 12 апреля 2018 г.

<sup>32</sup> “Hackers Interrupt Israeli Eurovision WebCast with Faked Explosions” (*«Хакеры прервали веб-трансляцию «Еurovision» в Израиле постановочными взрывами»*), BBC News, 15 мая 2019 г.; Zak Doffman, “Israel Responds to Cyber Attack with an Air Strike on Cyber Attackers in World First” (*«Израиль впервые в мире ответил на кибератаку воздушным ударом по киберпреступникам»*), Forbes, 6 мая 2019 г.

<sup>33</sup> David Hollis, “Cyberwar Case Study: Georgia 2008” (*«Анализ ситуации кибервойны: Грузия, 2008 г.»*), Small War Journal, 2010, доступно по ссылке: <https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.

<sup>34</sup> Andy Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar” (*«Как целая нация стала российской испытательной лабораторией для кибервойн»*), Wired, 20 июня 2017 г.; Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History” (*«Непассказанная история NotPetya, самой разрушительной кибератаки в истории»*), Wired, 22 августа 2018 г.

<sup>35</sup> Blake Johnson et al., “Attackers Deploy New ICS Attack Framework ‘TRITON’ and Cause Operational Disruption to Critical Infrastructure” (*«Злоумышленники предприняли атаку с помощью нового вируса ‘TRITON’ на систему управления предприятием, нарушив функционирование критической инфраструктуры»*), Fireeye Blogs, 14 декабря 2017 г.

соответствующими вооруженными конфликтами и, следовательно, подпадают ли они под действие МГП. Поступали также сообщения о кибероперациях, которые были предприняты Государствами в других ситуациях, правовая классификация которых может быть неоднозначной, в том числе осуществленных в так называемой «серой зоне».<sup>36</sup> Эти примеры свидетельствуют о росте интенсивности военных киберопераций за последнее десятилетие, то есть об изменении характера ведения войны – и эта тенденция может продолжиться. Действительно, поступают сведения о том, что все большее число Государств уже создали или находятся в процессе создания военного киберпотенциала, в том числе все пять постоянных членов Совета безопасности ООН.<sup>37</sup> Некоторые исследователи утверждали, что в более чем 100 странах действуют военные киберорганизации, хотя они существуют в разных формах и выполняют разные функции.<sup>38</sup> В этих условиях, исходя из гуманитарных соображений, принципиально важно изучать направления, в которых может продолжаться развитие и использование военного киберпотенциала в среднесрочной и долгосрочной перспективе.

В этом контексте необходимо принять во внимание отличия в характере ведения киберопераций во время военного конфликта и в мирное время. В общем и целом, военные ведомства Государств решают три главные задачи в киберпространстве. Во-первых, они отвечают за защиту военных сетей от вторжений со стороны всевозможных потенциальных источников угроз – от любопытного хакера-подростка, «идейных» хакеров и преступников до других Государств и их вооруженных сил. Поскольку военные силы и средства продолжают использовать интернет-каналы и встроены в информационную сеть, все большее значение приобретают имеющиеся у противников возможности эксплуатировать уязвимости в этих сетях для подрыва или нейтрализации военного потенциала. В некоторых Государствах такая ответственность за защиту военных сетей включает оказание поддержки более широкой общенациональной критической инфраструктуре, особенно во время кризиса. Вторая задача – это традиционная военная функция сбора и анализа разведанных о потенциальных противниках. Роль военных в добывании разведанных на государственном уровне может быть различной, иногда они делят эти обязанности со службами гражданской разведки, но вооруженным силам необходимо, как минимум, постоянно собирать информацию на поле боя. Именно в этом контексте необходимо проводить четкое различие между использованием военного киберпотенциала в мирное время и его использованием в ситуациях военного конфликта, имея в виду, помимо прочего, цели и характер такого использования. В-третьих, некоторым военным

<sup>36</sup> Например, в СМИ появлялись различные сообщения – основанные на информации из анонимных официальных источников – о том, что США проводили кибероперации против объектов в России и Иране и о том, что Израиль предпринял кибероперацию против морского порта в Иране. См. Ellen Nakashima, “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms” (*«Операция Управления киберопераций США нарушила доступ в интернет для российской фабрики троллей в день промежуточных выборов 2018 г.»*), *Washington Post*, 27 февраля 2019 г.; David E. Sanger and Nicole Perlroth, “U.S. Escalates Online Attacks on Russia’s Power Grid” (*«США наращивают интернет-атаки на энергосети России»*), *New York Times*, 15 июня 2019 г.; Julian E. Varnes and Thomas Gibbons-Neff, “U.S. Carried out Cyberattacks on Iran” (*«США предприняли кибератаку на Иран»*), *New York Times*, 22 июня 2019 г.; Joby Warrick and Ellen Nakashima, “Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility” (*«По сообщениям властей, Израиль причастен к парализующей кибератаке на портовое хозяйство Ирана»*), *Washington Post*, 18 мая 2020 г.

<sup>37</sup> Наряду с США и Великобританией, Франция поставила задачу «приобретения оборонительного киберпотенциала» для защиты от «зарубежных государств или террористических групп, [которые] могут атаковать элементы критической инфраструктуры». France, Agence Nationale de la Sécurité des Systèmes d’Information, *Information System Defence and Security: France’s Strategy* (*«Защита и безопасность информационных систем: стратегия Франции»*), 2011 г.. В Докладе о военной стратегии Китая 2015 г. заявлено, что «в ответ на ускоренное развитие военного киберпотенциала другими государствами Китай сформирует военно-оборонительный киберпотенциал». См. Government of China, *White Paper on China’s Military Strategy*, 2015. Россия не делала столь однозначных заявлений под данному вопросу, но «Доктрина информационной безопасности» Российской Федерации определяет «совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства» как одно из «основных направлений обеспечения информационной безопасности в области обороны страны». См. Министерство иностранных дел Российской Федерации, *Доктрина информационной безопасности Российской Федерации*, 5 декабря 2016 г.

<sup>38</sup> Shachtman Noah and Peter W. Singer, *The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Mislabeled and Counterproductive* (*Неправильная война: Настаивать на применении метафор холодной войны к кибербезопасности – неуместно и непродуктивно*), Brookings Institute, Washington DC, 2011.

киберструктурам поручено использовать национальную военную мощь в киберпространстве посредством наступательных киберопераций во время вооруженного конфликта. У таких операций могут быть как стратегические, так и тактические цели, включая системы вооружения противника, сети командования и управления или логистические центры. В конечном итоге ставится задача добиться физических и/или когнитивных результатов, которые способствуют достижению целей военной кампании и, как таковые, интегрируются в планирование и исполнение военных операций. Здесь также на пользу будущим обсуждениям пойдет точный анализ особенностей ведения Государствами киберопераций во время вооруженного конфликта по сравнению с операциями, проводимыми в мирное время, не в последнюю очередь с точки зрения качества и тяжести вредных последствий.

Примеры применения наступательных киберопераций во время конфликтов включают шпионаж; опознавание целей; информационные операции для воздействия на моральный дух противника и его готовность воевать; прерывание работы, обман или обфускацию систем связи противника с целью нарушить координацию сил и средств; и кибероперации в поддержку кинетических операций.<sup>39</sup> Примером последнего служит подавление военных радиолокационных станций противника для обеспечения авиационных ударов.<sup>40</sup> Этот неисчерпывающий перечень заставляет поставить вопрос, касающийся стратегических и тактических задач, которые военные могут стремиться решать посредством киберактивности в вооруженном конфликте; это позволит достичь более глубокого понимания будущего характера киберконфликтов. В частности, необходимо более детально изучить то, как может выглядеть в ближайшем будущем “кибервойна” в ее более узкой трактовке – как длящегося военного противостояния хорошо подготовленных субъектов «внутри» киберпространства – и как такие сценарии могут по-разному развиваться в зависимости от того, оказываются ли военные в ситуации симметричного или асимметричного конфликта.

---

<sup>39</sup> ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, (*Недопущение причинения вреда гражданскому населению от военных киберопераций во время вооруженных конфликтов*) – готовится к выпуску.

<sup>40</sup> Sharon Weinberger, “How Israel Spoofed Syria’s Air Defense System” (*«Как Израиль обманул систему ПВО Сирии»*), *Wired*, 4 октября 2007 г.; Lewis Page, “Israeli Sky-Hack Switched Off Syrian Radars Countrywide” (*«Израильский Sky-Hack отключил сирийские радары по всей стране»*), *The Register*, 22 ноября 2007 г.

## Женевская академия международного гуманитарного права и прав человека

Женевская академия обеспечивает последипломное образование, проводит академические исследования в области права и политики, организует учебные курсы и совещания экспертов. Мы сосредоточены на отраслях международного права, которые имеют отношение к ситуациям вооруженного конфликта и затяжного насилия и к защите прав человека.

Женевская академия  
международного гуманитарного  
права и прав человека

Villa Moynier  
Rue de Lausanne 120B  
CP 1063 - 1211 Geneva 1 - Switzerland  
Phone: +41 (22) 908 44 83  
Email: [info@geneva-academy.ch](mailto:info@geneva-academy.ch)  
[www.geneva-academy.ch](http://www.geneva-academy.ch)

© The Geneva Academy of International  
Humanitarian Law and Human Rights

Данная работа доступна для  
использования по лицензии Creative  
Commons - с указанием авторства –  
некоммерческая – с сохранением  
условий, версия 4.0 Международная  
(CC BY-NC-ND 4.0)



